



PRONOVA

SOLUÇÕES
INTELIGENTES



(12/11/2008)

Pronova Consultoria em Tecnologia da Informação Ltda. & Feitian Technologies Co., Ltd.

Contrato de Uso de Software

Todos os produtos da FEITIAN Technologies Co., Ltd. (FEITIAN) e Pronova Soluções Inteligentes (PRONOVA) incluindo, sem limitar-se a, cópias de avaliação, disquetes, CD-ROMs, hardware, software e documentação, e todos os futuros pedidos, estão sujeitos aos termos desta Licença. Se você não está de acordo com os termos aqui expostos, por favor, proceda a devolução do pacote completo e dentro do prazo de quinze dias úteis e reembolsaremos o custo do produto, exceto o frete e os encargos administrativos. Ao utilizar o produto você declara conhecer e aceitar os termos e condições do presente, que se formalizará em um contrato de Licença entre você e a FEITIAN, que também terá alcance aos distribuidores, revendas ou representantes da FEITIAN, com o alcance aqui convencionado.

1. **Uso Permitido** – Você pode fundir, relacionar e/ou fazer link do Software com outros programas com o único propósito de proteger esses programas de acordo com o uso descrito no Guia do Desenvolvedor que está junto com o produto, ou que pode ser encontrado no site web da FEITIAN (www.ftsafes.com) ou da PRONOVA (www.pronova.com.br). Você pode realizar cópias do Software com o fim de utilizá-las como cópias de segurança ou backup.

2. **Uso proibido** – O Software ou o hardware fornecido pela FEITIAN/PRONOVA ou qualquer outra parte do Produto não pode ser reproduzida, copiada, reinventada, desassemblada, descompilada, revisada, melhorada e modificada de qualquer forma, exceto como especificamente se permite no presente. Você não pode praticar engenharia reversa ao Software ou qualquer parte do produto, ou tentar descobrir o código fonte do Software. Você não pode usar o meio ótico ou magnético incluído com o produto com o propósito de transferir ou guardar dados que não fazem parte original de Produto, ou uma melhora ou atualização de Produto fornecida pela FEITIAN ou pela PRONOVA.



O equipamento obedece ao principal requerimento de proteção da Diretiva EMC (Diretiva 89/336/EEC relativa à compatibilidade eletromagnética) baseada em um teste voluntário.

Este certificado se refere somente a um exemplo particular do produto e a documentação técnica deste fornecida para teste e certificação. Os resultados detalhados e todos os padrões usados, bem como o modo de operação estão listados em:

Relatório Teste No. 70407310011
Testes Realizados EN 55022/1998 EN 55024/1998

Após a preparação da documentação técnica necessária, bem como a declaração de conformidade CE a marca exibida acima pode ser fixado no equipamento como estipulado no Artigo 10.1 da Diretiva. Outras diretivas relevantes devem ser observadas.

Certificado de Aprovação FCC



Este dispositivo está em conformidade com a Parte 15 das Regras FCC e Regulamentações para Equipamentos de Tecnologia da Informação.



Este equipamento está baseado nos padrões USB.

WEEE (Waste Electrical and Electronic - Descarte de Equipamentos Elétricos e Eletrônicos)



A Diretiva Europeia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É sua responsabilidade eliminar este e qualquer outro equipamento elétrico e eletrônico através dos postos de recolhimento designados pelas autoridades governamentais ou locais. A eliminação e reciclagem correta ajudarão a prevenir as consequências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o seu equipamento antigo, entre em contato com as autoridades locais, serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

Programa Logo Microsoft Windows



Este dispositivo foi aprovado nos testes Windows HCT, realizados nos Laboratórios de Provas de Hardware Windows (WHQL), os quais determinam que os produtos atendem a todos os requisitos do Programa de Logos do Windows.

Check Point OPSEC



O Token USB ePass possuem a certificação OPSEC (Open Platform for Security) da Check Point Software Technologies Ltd. (NASDAQ: CHKP), líder mundial em segurança através de Internet. Com a certificação OPSEC, o Token USB ePass se integra de forma transparentemente com as soluções líderes da Check Point do mercado: VPN-1®, FireWall-1® e Next-Generation®.

Entrust Ready



Os Tokens ePass são dispositivos criptográficos seguros e portáteis, ideais para Entrust/PKI e outras aplicações tais como: autenticação de dois fatores, codificação de e-mail, sites seguros (SSL), logon VPN e muito mais. Foi outorgado aos Tokens ePass o status Entrust Ready com as aplicações o Entrust Entelligence client e Entrust Authority Security Manager.

As informações contidas neste manual estão sujeitas a alterações sem aviso prévio e não representam um compromisso por parte de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA. Nenhuma parte deste manual poderá ser reproduzida de qualquer forma ou meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou sistemas de armazenamento e recuperação, sem o prévio consentimento, por escrito, de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA.

Windows® é marca registrada da Microsoft Corporation

Pentium® é marca registrada da Intel Corporation

ePassNG é marca registrada da Feitian Technologies Inc., Ltd.

ROCKEY é marca registrada da Feitian Technologies Inc., Ltd.

AMD® é marca registrada da Advanced Micro Devices

PROTOKEN é marca registrada da Pronova Soluções Inteligentes

Índice

POLÍTICA DE GARANTIA PRONOVA	7
1. Glossário	11
2. Lista de Acrônimos	14
3. Sobre a Pronova Soluções Inteligentes	16
4. Sobre a Feitian Technologies Inc., Ltd.	16
5. Sobre o Token USB Protoken NG	16
5.1 Especificações Técnicas (requisito FIPS 140-2, item 4.1)	17
5.2 Requisitos mínimos do sistema:	17
5.3 Vantagens do Token USB Protoken NG	18
5.4 Recursos do Hardware	18
5.5 Arquitetura (requisito FIPS 140-2, item 4.1)	19
6. Instalando o software do Token USB Protoken NG	20
6.1 Instalação nos sistemas operacionais Windows 2000, Windows XP, Windows Vista e Windows 2003	20
6.2 Instalação nos sistemas operacionais Windows 98SE e Windows ME	22
6.3 Configurando o Tempo de Vida do PIN do Protoken NG	23
7.1 Como alterar o PUK?	24
8. O que é o PIN do Usuário? (requisito FIPS 140-2, item 4.3.1)	26
8.1 Destravando o PIN do Usuário	28
9. Formatando o Setor PKI do Protoken NG	30
10. Instalando um certificado emitido por uma AC Microsoft no Protoken NG	32
11. Integrando o Protoken NG com o Mozilla Firefox 1.5	34
12. Utilizando o Firefox 1.5 para alterar o PIN do Usuário do Protoken NG	37
13. Importando um certificado para o Protoken NG a partir de um arquivo	39
14. Configurando o Microsoft Outlook para usar um certificado armazenado no Protoken NG	42
15. Configurando o Outlook Express para usar um certificado armazenado no Protoken NG	44
16. Integrando o Protoken NG com o Mozilla Thunderbird	50
17. Configurando sua conta de e-mail no Mozilla Thunderbird para fazer uso do certificado digital armazenado no Protoken NG	51
18. Adicionando a identidade digital do remetente ao catálogo de endereços do Windows...52	
19. Enviando uma mensagem criptografada usando o Outlook Express.....54	
20. Adicionando uma identificação digital à sua lista de contatos do Microsoft Outlook.....57	
21. Enviar uma mensagem com uma assinatura digital para um destinatário da Internet usando o Microsoft Outlook.....59	
22. Enviar uma mensagem criptografada para um destinatário da Internet usando o Microsoft Outlook	59
23. Removendo o software do Protoken NG	60
24. Perguntas e Respostas Comuns	60
25. Suporte Técnico	62
26. Contatos	62

POLÍTICA DE GARANTIA PRONOVA

IMPORTANTE-LEIA ESTA GARANTIA DO FABRICANTE COM ATENÇÃO PARA ENTENDER SEUS DIREITOS E OBRIGAÇÕES! O termo "Dispositivo de Hardware" significa o produto de hardware Pronova. O termo "Você" significa uma pessoa física ou jurídica que será referida nesta Garantia Limitada como "Você" e "Seu(s)/Sua(s)".

A. GARANTIAS.

1. Garantia Expressa. Você estará sujeito aos termos e condições desta Garantia Limitada e, em substituição a quaisquer outras (se houver) garantias expressas, a Pronova garante a Você, sob condições normais de uso e serviço, na data da aquisição identificada no recibo ou no comprovante de pagamento e pelo período de tempo especificado abaixo para o Dispositivo de Hardware aplicável (doravante denominados o "Prazo de Garantia"), que o Dispositivo de Hardware será executado substancialmente em conformidade com o descrito na embalagem e na documentação da Pronova que o acompanha.

A PRONOVA assegura total cobertura contra defeito de fabricação para os produtos fornecidos ao cliente no território brasileiro, durante o período da garantia.

Prazo de Garantia

Garantia Legal - 90 (noventa) dias

A garantia legal praticada pela PRONOVA obedece aos dispositivos relacionados no artigo 26 do Código de Defesa do Consumidor (CDC), e é direito do consumidor que apresente a reclamação comprovadamente formulada no prazo de 90 (noventa) dias da data de aquisição do produto PRONOVA para troca do produto e/ou serviço adquirido por igual ou equivalente superior.

A reposição dos produtos em garantia estará sujeita às condições de retorno do produto, observando a garantia legal, conforme art. 50 do CDC.

PRAZO TOTAL DA GARANTIA:

- (I) Para todos os conjuntos de Tokens USB: 90 (noventa) dias;
- (II) Leitor de cartão inteligente: 90 (noventa) dias;
- (III) Cartão Inteligente: 90 (noventa) dias.
- (IV) Dongles para proteção de software: 90 (noventa) dias.

Os dispositivos criptográficos (tokens e cartões) e leitores de cartão inteligente vendidos pela PRONOVA tem garantia contra defeitos de fabricação pelo prazo de 90 (noventa) dias contados a partir da data de aquisição do produto PRONOVA.

Os dispositivos criptográficos (tokens e cartões) armazenam o seu Certificado Digital protegendo-o contra acessos indevidos. AS SENHAS (PIN, PUK, SENHA, FRASE SENHA OU PASSWORD) PARA ACESSO A ESSES DISPOSITIVOS SÃO SOMENTE DE CONHECIMENTO E RESPONSABILIDADE DO TITULAR OU RESPONSÁVEL DO CERTIFICADO DIGITAL, E A PRONOVA NÃO MANTÉM CÓPIAS OU POSSUI MEIOS DE RECUPERÁ-LAS.

CASO O DISPOSITIVO CRIPTOGRÁFICO SEJA BLOQUEADO OU INUTILIZADO DEVIDO À PERDA DAS SENHAS, SEU CONTEÚDO SERÁ PERDIDO. A REPOSIÇÃO DESTES DISPOSITIVOS (E DE SEU CONTEÚDO) NÃO É COBERTA PELA POLÍTICA DE GARANTIA PRONOVA.

Caso o Serviço de Suporte Técnico PRONOVA constate defeito de fabricação que requeira a substituição do dispositivo criptográfico durante o período de vigência desta garantia, a PRONOVA:

- Efetuará troca do dispositivo criptográfico, sem custo adicional para o cliente; e
- Não emitirá um novo certificado, sem custo adicional para o cliente, caso o defeito de fabricação acarrete na perda do Certificado Digital.

Essa Garantia Limitada não cobrirá, bem como não será fornecido qualquer tipo de garantia para aspectos subjetivos ou estéticos do Dispositivo de Hardware. A garantia expressa prevista acima constitui a única garantia expressa concedida a Você e é fornecida em substituição a todas as outras condições e garantias, sejam expressas ou implícitas (exceto quaisquer garantias implícitas existentes que não possam ser recusadas), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Qualquer informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, não criará qualquer garantia ou condição ou ampliará o escopo desta Garantia Limitada.

2. Limitação da Vigência das Garantias Implícitas. Se Você for um consumidor estrangeiro, também poderá ter uma condição e/ou garantia implícita de acordo com a legislação de algumas jurisdições, a qual é limitada pela vigência do presente Prazo de Garantia.

B. RECURSO EXCLUSIVO. Sujeito à legislação aplicável e às disposições a seguir, e desde que Você, durante o Prazo de Garantia, devolva o Dispositivo de Hardware à Pronova, com uma cópia do recibo ou comprovante válido de pagamento, a Pronova irá, a seu critério:

(i) reparar ou substituir o Dispositivo de Hardware; ou (ii) indenizá-lo pelos danos diretos sofridos por Você, limitando-se a responsabilidade ao valor efetivamente pago por Você pelo Dispositivo de Hardware.

(ii) Qualquer Dispositivo de Hardware reparado ou substituído conforme esta Garantia Limitada terá garantia pelo Prazo de Garantia original remanescente ou por 30 (trinta) dias, a partir da data de devolução do item para Você, o que for maior.

Salvo previsão expressa em contrário pela legislação aplicável, Você deverá arcar com os custos relacionados ao transporte (inclusive embalagem) do produto dentro do prazo da garantia; e

C. ISENÇÃO DE OUTRAS GARANTIAS. A garantia expressa especificada acima é a única garantia expressa oferecida a Você e é fornecida em substituição a todas as outras condições e garantias expressas ou implícitas (se houver), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Nenhuma outra garantia é fornecida em relação ao Dispositivo de Hardware ou aos serviços de garantia por qualquer pessoa, incluindo, mas não se limitando a, a Pronova, os seus agentes, as afiliadas e os fornecedores. Nenhuma informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, deverá criar uma garantia ou condição ou ampliar o escopo desta Garantia Limitada. Também não há garantias ou condições de titularidade, uso pacífico ou não-violação de direitos de autor no Dispositivo de Hardware.

D. EXCLUSÃO DE OUTROS DANOS.

NA EXTENSÃO MÁXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, A PRONOVA, SEUS AGENTES, AFILIADAS E/OU FORNECEDORES NÃO SERÃO RESPONSÁVEIS POR QUALQUER:

(i) DANO CONSEQÜENCIAL OU INCIDENTAL;

(ii) DANOS POR LUCROS CESSANTES, INTERRUPTÃO DE NEGÓCIOS, PERDA DE DADOS, INFORMAÇÕES CONFIDENCIAIS OU OUTRAS, PERDA DE PRIVACIDADE, QUALQUER INABILIDADE NO USO DO DISPOSITIVO DE HARDWARE, NO TODO OU EM PARTE, DANOS PESSOAIS OU QUALQUER FALHA NO CUMPRIMENTO DE QUALQUER OBRIGAÇÃO (INCLUINDO MAS NÃO SE LIMITANDO A QUALQUER

OBRIGAÇÃO GERADA EM RELAÇÃO A CASO DE NEGLIGÊNCIA E QUEBRA DO PRINCÍPIOS DE BOA-FÉ E DO ESFORÇO DE APRIMORAMENTO);

(iii) DANO INDIRETO, ESPECIAL OU PUNITIVO DECORRENTE DO OU DE QUALQUER FORMA RELACIONADO COM O DISPOSITIVO DE HARDWARE.

(iii) QUALQUER TIPO DE INFORMAÇÃO QUE VENHA A SER ARMAZENADA NOS EQUIPAMENTOS COMERCIALIZADOS PELA PRONOVA.

AS EXCLUSÕES ACIMA SERÃO APLICADAS MESMO QUE A PRONOVA OU QUALQUER AGENTE, AFILIADA OU FORNECEDOR TENHA SIDO ALERTADO SOBRE A POSSIBILIDADE DE OCORRÊNCIA DE TAIS PERDAS OU DANOS, E MESMO QUE HAJA FALHA, DANO (INCLUSIVE NEGLIGÊNCIA), RESPONSABILIDADE OBJETIVA OU PELO FATO DO PRODUTO, DECLARAÇÃO FALSA OU QUALQUER OUTRO MOTIVO.

E. EXCLUSÕES DE COBERTURA. A Garantia Limitada não será aplicável e a Pronova, seus agentes, afiliadas e/ou fornecedores não terão qualquer responsabilidade relativa a esta Garantia Limitada se o Dispositivo de Hardware:

(i) for usado para fins comerciais (inclusive aluguel ou arrendamento);

(ii) for modificado ou adulterado;

(iii) for danificado por motivos de força maior, alta-tensão, uso indevido, abuso, negligência, acidente, desgaste, manipulação indevida, aplicação errada ou outras causas não relacionadas a defeitos no Dispositivo de Hardware;

(iv) for danificado por programas, informações, vírus ou arquivos ou durante envios ou transmissões;

(v) não for usado de acordo com a documentação e as instruções de uso que o acompanham; ou

(vi) for reparado, modificado ou alterado por outra pessoa que não seja um representante da assistência técnica autorizada da Pronova e se a assistência técnica não autorizada causar ou contribuir para o surgimento de qualquer defeito ou dano.

F. REGISTRO. Não é necessário registrar a aquisição do Dispositivo de Hardware para que essa Garantia Limitada tenha validade.

G. BENEFICIÁRIO. Na extensão máxima permitida pela lei aplicável, a Garantia Limitada será concedida exclusivamente a Você, o primeiro adquirente do Dispositivo de Hardware, não existindo outros beneficiários da Garantia Limitada. Salvo previsão expressa em contrário na lei, esta Garantia limitada não será destinada, bem como não será aplicável a qualquer outra pessoa, inclusive qualquer pessoa para a qual Você faça uma transferência do Dispositivo de Hardware.

H. INFORMAÇÕES ADICIONAIS. A Pronova é a entidade que fornece esta Garantia Limitada. Para receber instruções sobre como executar esta Garantia Limitada, entre em contato com uma subsidiária Pronova de sua localidade ou escreva para; Pronova Soluções Inteligente, Avenida das Américas 500, bloco 4, sala 302, Barra da Tijuca, Rio de Janeiro, RJ, CEP 22.640-100, ou visite a Pronova na Internet no endereço <http://www.pronova.com.br>

Outras exigências:

1. Você deverá enviar um comprovante de pagamento na forma de uma fatura (ou uma cópia) ou um recibo autêntico com data evidenciando que Você é o beneficiário desta Garantia Limitada e que a Sua solicitação está sendo feita dentro do Prazo de Garantia.

2. Para execução da Garantia Limitada, Você deverá levar ou enviar o item na sua embalagem original ao local especificado pela Pronova. Salvo previsão expressa em contrário prevista na legislação aplicável, Você arcará com os custos relacionados ao

transporte (inclusive embalagem) do serviço dentro do prazo da garantia.

Caso não siga as instruções acima, Você poderá ter despesas adicionais, poderá perder a sua garantia ou poderão ocorrer atrasos.

As informações contidas neste documento, incluindo URLs e outras referências a sites na Internet, estão sujeitas a alterações sem aviso prévio. Salvo indicação em contrário, os exemplos de empresas, organizações, produtos, nomes de domínio, endereços de email, logotipos, pessoas, lugares e acontecimentos aqui mencionados são fictícios e nenhuma associação com qualquer empresa, organização, produto, nome de domínio, endereço de e-mail, logotipo, pessoa ou acontecimento real é intencional ou deve ser inferida.

Obedecer a todas as leis de direitos autorais aplicáveis é responsabilidade do usuário. Sem limitar os direitos autorais, nenhuma parte deste documento pode ser reproduzida, armazenada ou introduzida em um sistema de recuperação, ou transmitida de qualquer forma por qualquer meio (eletrônico, mecânico, fotocópia, gravação ou qualquer outro), ou para qualquer propósito, sem a permissão expressa e por escrito da Pronova.

A Pronova pode ter patentes ou requisições para obtenção de patente, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual que abrangem o conteúdo deste documento. A posse deste documento não lhe confere nenhum direito sobre as citadas patentes, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual, salvo aqueles expressamente mencionados em um contrato de licença, por escrito, da Pronova.

© 2004 Pronova Soluções Inteligentes. Todos os direitos reservados.

ePass, ePassNG, EnterSafe, ePass1000, ePass2000, ePass3000, Rockey e BioPass3000 são marcas registradas ou comerciais da Feitian Technologies Co., Inc. na República Popular da China e/ou em outros países.

Pronova e ProToken são marcas registradas ou comerciais da Pronova Consultoria em Tecnologia da Informação Ltda. na República Federativa do Brasil e/ou em outros países.

Os nomes de produtos e de empresas reais aqui mencionados podem ser marcas comerciais de seus respectivos proprietários.

A Pronova concede ao comprador deste produto o direito de reproduzir uma (1) cópia do "Manual de Instruções" impresso para cada Dispositivo de Hardware adquirido na embalagem.

1. Glossário

Assinatura Digital: Resultado de uma transformação criptográfica de dados, que quando implementada apropriadamente, provê os seguintes serviços de segurança: autenticação da origem, integridade de dados e não repudição do signatário.

Atribuição de chaves (key establishment): Processo que possibilita atribuir uma chave simétrica para uso criptográfico aos participantes legítimos de uma sessão de comunicação. A atribuição de chaves pode ser realizada por meio de duas técnicas: “Negociação de Chaves” ou “Transferência de Chaves”.

Autoridade Certificadora (AC): Entidade idônea autorizada a emitir, renovar e cancelar certificados digitais. É responsável pela administração das chaves públicas.

Autoridade de Registro (AR): É uma entidade operacionalmente vinculada à determinada Autoridade Certificadora Habilitada, responsáveis pela confirmação da identidade dos solicitantes dos certificados e-CPF e e-CNPJ.

Certificado Digital: Documento eletrônico assinado digitalmente por uma autoridade certificadora, e que contém diversos dados sobre o emissor e o seu titular. A função precípua do certificado digital é a de vincular uma pessoa ou uma entidade a uma chave pública.

Chave criptográfica: Código ou parâmetro usado em conjunto com um algoritmo criptográfico, determinando as seguintes operações:

- Transformação de dados em texto claro para um formato cifrado e vice-versa;
- Assinatura digital computada a partir de dados;
- Verificação de uma assinatura digital computada a partir de dados;
- Geração de um código de autenticação computado a partir de dados; ou
- Um acordo para troca de um segredo compartilhado.

Chave Criptográfica em texto claro: representa uma chave criptográfica não cifrada.

Chave secreta: Chave criptográfica, usada com um algoritmo criptográfico de chave secreta, que está unicamente associada a uma ou mais entidades e não deveria tornar-se pública.

Código de Autenticação: corresponde a um verificador de integridade criptográfico que é comumente referenciado como MAC (Message Authentication Code).

Co-assinatura: A co-assinatura (ou sign) é aquela gerada independente das outras assinaturas.

Contra-assinatura: A contra-assinatura (ou countersign) é aquela realizada sobre uma assinatura já existente. Na especificação PKCS#7, a contra-assinatura é adicionada na forma de um atributo não autenticado (countersignature attribute) no bloco de informações (signerInfo) relacionado a assinatura já existente.

Elemento de Dado: Corresponde a um item de informação para o qual são definidos um nome, uma descrição de conteúdo lógico, um formato e uma codificação [ISO/IEC 7816-4].

Entidade usuária externa: Um indivíduo ou processo que realiza acesso a um módulo criptográfico independentemente do papel assumido.

Protoken NG: Dispositivo criptográfico portátil integrado com smart card e porta USB, o qual foi desenvolvido pela Feitian. Uma das vantagens deste dispositivo sobre os cartões inteligentes é a portabilidade, bem como suporte a aplicações PKI.

ePassNG: Nova geração de produto (middleware framework) desenvolvido pela Feitian. Este novo middleware suporta todas as séries dos produtos ePass. Fácil de ser atualizado com novo suporte de hardware, bem como suporte a aplicações PKI.

FIPS (Federal Information Processing Standards): correspondem a padrões e diretrizes desenvolvidos e publicados pelo NIST (National Institute of Standards and Technology) para uso de sistemas computacionais no âmbito governamental federal norte-americano. O NIST desenvolve os padrões e diretrizes FIPS, quando há requisitos obrigatórios do governo federal, tais como, segurança e interoperabilidade, e não há padrões ou soluções industriais aceitáveis.

Firmware: Programas e componentes de dados de um módulo que estão armazenados em hardware (ROM, PROM, EPROM, EEPROM ou FLASH, por exemplo) e não podem ser dinamicamente escritos ou modificados durante a execução.

Fronteira criptográfica (cryptographic boundary): A fronteira criptográfica é um perímetro explicitamente definido que estabelece os limites físicos de um módulo criptográfico.

Hardware: Parte ou equipamento físico usado para processar programas e dados.

ICP-Brasil: conjunto de técnicas, práticas e procedimentos, a ser implementado pelas organizações governamentais e privadas brasileiras com o objetivo de garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Identificador de Registro: Valor associado a um registro que pode ser usado para referenciar aquele registro. Diversos registros poderiam ter o mesmo identificador dentro de um EF [ISO/IEC 7816-4].

Integridade: propriedade que determina que dados não devem ser modificados ou apagados de uma maneira não autorizada e indetectável.

Interface: representa um ponto lógico de entrada e saída de dados, que provê acesso aos serviços disponíveis pelos módulos criptográficos.

Interface CryptoAPI: Interface de operação de criptografia desenvolvida pela Microsoft. Esta interface oferece ao dispositivo idempendência ou implementação de encapsulamento de algoritmos criptográficos, permitindo aos desenvolvedores uma fácil utilização destes algoritmos em suas aplicações PKI, incluindo criptografia de dados, verificação de certificados e assinatura digital na plataforma Windows.

ITI: autarquia federal vinculada à Casa Civil da Presidência da República. O ITI é a Autoridade Certificadora Raiz - **AC Raiz** da Infra-Estrutura de Chaves Públicas Brasileira - **ICP-Brasil**. Como tal é a primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil.

Middleware: Software que é usado amarrar uma aplicação.

Módulo criptográfico (cryptographic module): Conjunto de hardware, software e/ou firmware que implementa funções ou processos criptográficos, abrangendo algoritmos criptográficos e de geração de chaves.

Módulo criptográfico de chip único (Single-chip Cryptographic Module): representa uma materialização física na qual um chip único de circuito integrado (Integrated Circuit Chip - ICC) poderia ser usado como dispositivo independente (standalone), ou poderia estar embutido/confinado dentro de um produto (material de área delimitada), que está ou não fisicamente protegido. Por exemplo, módulos criptográficos de chip único incluem os cartões inteligentes (Smart Cards).

Negociação de chaves (key agreement): Protocolo que possibilita atribuir uma chave simétrica aos participantes legítimos em função de valores secretos definidos por cada um dos participantes, de forma que nenhum dos participantes possa predeterminar o valor da chave. Neste método, a chave não é transferida, nem mesmo de forma cifrada. Exemplo

clássico desta classe de protocolo é o algoritmo Diffie-Hellman.

Número de Identificação Pessoal (Personal Identification Number - PIN): um código alfanumérico ou senha usada para autenticar uma identidade.

Número de Registro: Número seqüencial atribuído a cada registro, que serve para identificar unicamente o registro dentro de seu EF [ISO/IEC 7816-4].

Oficial de segurança: uma entidade ou processo que age como tal, realizando funções criptográficas de iniciação ou gerenciamento.

Parâmetros críticos de segurança (PCS): Representam informações sensíveis e relacionadas a segurança, tais como, chaves criptográficas privadas, chaves simétricas de caráter secreto, chaves de sessão e dados de autenticação (senhas e PIN, por exemplo), cuja divulgação ou modificação podem comprometer a segurança de um módulo criptográfico.

PC/SC: especificação para integração de cartões inteligentes (smart card) em sistemas de computação

PKCS#11: padrão utilizado como interface para invocar operações criptográficas em hardware e é utilizado para prover suporte aos tokens.

Registro: Cadeia (string) de bytes que pode ser manuseada como um todo pelo cartão inteligente e referenciada por um número de registro ou por um identificador de registro [ISO/IEC 7816-4].

Senha: uma cadeia de caracteres (letras, números e outros símbolos) usada para autenticar uma identidade ou para verificar autorizações de acesso.

Software: Programas e componentes de dados usualmente armazenados em mídias que podem ser apagadas (disco rígido, por exemplo), os quais podem ser dinamicamente escritos e modificados durante a execução.

Token: Nome geral de todos os dispositivos criptográficos, tais como cartões inteligentes (smart cards), dispositivos que possuem senhas e funcionalidades de armazenamento de certificados etc.

Token USB: Dispositivo criptográfico com conector USB, portátil e de fácil uso.

TSP (Token Service Provider): Camada de hardware abstrata presente no framework ePassNG. Esta camada interfaces comuns de entrada e saída para todos os tipos de dispositivos. O design pode prover uma determinada expansão contra as diferenças de hardware.

Transporte de chaves (key transport): Protocolo que possibilita que uma chave simétrica seja transferida aos participantes legítimos da entidade geradora para parceiros. Neste método, a chave é definida por uma das entidades e repassada para as demais.

Unidade de Dado: O menor conjunto de bits que pode ser referenciado de forma não ambígua [ISO/IEC 7816-4].

Usuário: um indivíduo ou processo que age como tal com o intuito de obter acesso a um módulo criptográfico para executar serviços.

2. Lista de Acrônimos

AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
ATR	Answer To Reset
CBC	Cipher Block Chaining
CE	Consumer electronics
CFCA	China Financial Certificate Authority
CLK	Clock
DES	Data Encryption Standard
DF	Dedicated File
EEPROM	Electrically Erasable Programmable Read-Only Memory
EF	Elementary File
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GND	Ground
ICC	Integrated Circuit Chip
ICP	Infra-Estrutura de Chaves Públicas
ICP-Brasil	Infra-Estrutura de Chaves Públicas Brasileira
IEC	International Electrotechnical Commission
IKE	Internet key exchange
IN	Instrução Normativa
IPSec	Internet Protocol Security
I/O	Input/Output
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
ITI	Instituto Nacional de Tecnologia da Informação
IV	Initialization Vector
JCE	Java Cryptography Extension

LCR Lista de Certificados Revogados

LEA Laboratório de Ensaios e Auditoria

LSITEC Laboratório de Sistemas Integráveis Tecnológico

MAC Message Authentication Code

MF Master File

MSCAPI Microsoft Crypto API

NIST National Institute of Standards and Technology

OPSEC Operations security

PC Personal Computer

PCS Parâmetros Críticos de Segurança

PIN Personal Identification Number

PPS Protocol and Parameters Selection

PUK PIN Unlock Key

RFU Reserved for Future Use

RNG Random Number Generator

RSA Rivest Shamir and Adleman

RST Reset

SHA Secure Hash Algorithm

SO Sistema Operacional

SP Service Provider

SSL Secure Sockets Layer

TLV Tag Length Value

TSP Token Service Provider

TTL Time To Live

USB Universal Serial Bus

VPP Variable Supply Voltage

3. Sobre a Pronova Soluções Inteligentes

A Pronova Soluções Inteligentes é formada por uma equipe com mais de 15 anos de experiência no mercado de Segurança da Informação. Somos pioneiros neste setor, no qual sempre nos destacamos pela qualidade dos produtos que oferecemos aliada ao bom atendimento, formação de parcerias, lançamento de novas tecnologias, além de serviços de consultoria.

Ao longo deste período, lançamos e comercializamos no Brasil produtos desenvolvidos e utilizados em larga escala no mercado internacional. Atendemos as mais variadas necessidades de proteção, como armazenamento e transmissão segura de informações, monitoramento de conteúdo hostil, além de proteção de software contra pirataria, entre outros.

4. Sobre a Feitian Technologies Inc., Ltd.

A Feitian Technologies Co., Ltd. iniciou suas operações em 1998 com o desenvolvimento do Sistema de Proteção de Software ROCKEY. Ao longo de suas atividades, a Feitian se tornou rapidamente o principal provedor de chaves de proteção de software na China e aumentou exponencialmente suas vendas no mercado mundial.

5. Sobre o Token USB Protoken NG

O **Protoken NG** é um token USB que foi desenvolvido para oferecer autenticação, verificação e serviços de criptografia de informações, além de suporte para criptografia de e-mails, assinatura digital e uso de SSL no Internet Explorer, Outlook, Outlook Express, Netscape Communicator ou qualquer outro software baseado em padrões Microsoft Crypto API ou PKCS#11. Como os demais produtos existentes no mercado, o Protoken NG é notavelmente versátil e pode ser usado para criar diversas outras aplicações.

O **Protoken NG** é um token USB de autenticação que pode ser utilizado em Windows 98SE, 2000, ME, XP, Vista, 2003, MacOS 8/9 e Linux. Da mesma forma que um cartão inteligente (smart card), pode executar poderosos cálculos de criptografia.

A seguir os principais recursos oferecidos pelo Token USB Protoken NG

- Geração no próprio dispositivo (on board) do par de chaves RSA 1024 e 2048bits;
- Suporte nativo para os algoritmos RSA, MD5, SHA1, DES e 3DES;
- Suporte padrão para aplicações Microsoft Crypto API;
- Compatível com Windows 2000 PC/SC;
- Geração de números aleatórios em hardware;
- Assinatura digital realizada em hardware;
- Suporte para múltiplas aplicações PKI, inclusive ICP-Brasil;
- Suporte para múltiplos armazenamentos de chaves e certificados;
- Interface padrão USB tipo A compatível com 2.0;
- Certificações CE, FCC, CFCA, OPSEC e FIPS;
- Chassi de plástico resistente (tamper evident); resistente a água;
- Capa protetora do conector USB;
- Gerenciamento através de um PIN e de um PUK;
- Software de Instalação, Gerenciamento e Teste do dispositivo em Português do Brasil.

5.1 Especificações Técnicas (requisito FIPS 140-2, item 4.1)

Sistemas Operacionais:	Windows 98SE, 2000, ME, XP, Vista, 2003, MacOS (PowerPC e Intel) e Linux (kernel 2.4 ou mais recente)
Certificações e Padrões:	PKCS#11 v2.10, MS CAPI, PC/SC, X.509 v3, SSL v3, IPSec/IKE, ISO 7816 3-4, FCC, CE, CFCA, OPSEC e FIPS 140-2
Processador:	32bits
Memória Disponível:	128KB (sendo que disponível para o usuário final 64KB)
Algoritmos On-Board:	RSA, DES, 3DES, DAS, MD5 e SHA-1
Nível de Segurança do Chip:	Armazenamento de dados seguro e criptografado
Dimensões:	58x19x8 mm (com a capa do conector USB) 55x19x8 mm (sem a capa do conector USB)
Peso:	9g
Dissipação de Energia:	< 250 mW
Temperatura de Operação:	0 até 70°C
Temperatura de Armazenamento:	-40 até 85°C
Faixa de umidade:	0 até 100% - 0 até 100% sem condensação
Conector:	Universal Serial Bus, tipo A compatível com 2.0
Chassi:	Plástico reforçado, à prova de violação (tamper evident)
Retenção de Dados de memória:	Pelo menos 10 anos
Capa protetora do conector USB	Sim
Número Serial impresso no chassi	Sim

5.2 Requisitos mínimos do sistema:

Para que seja possível fazer uso do Protoken NG, verifique se seu sistema possui os seguintes requisitos mínimos:

Sistema Operacional	Windows 98SE, ME, 2000, 2003, XP, Vista MacOS (Power PC ou Intel) ou Linux (kernel 2.4 ou mais recente)
Espaço em disco	Pelo menos 10 MB
Porta USB	Pelo menos uma porta USB tipo A livre
Direitos	O usuário deverá ter direito de instalar dispositivos no sistema operacional

5.3 Vantagens do Token USB Protoken NG

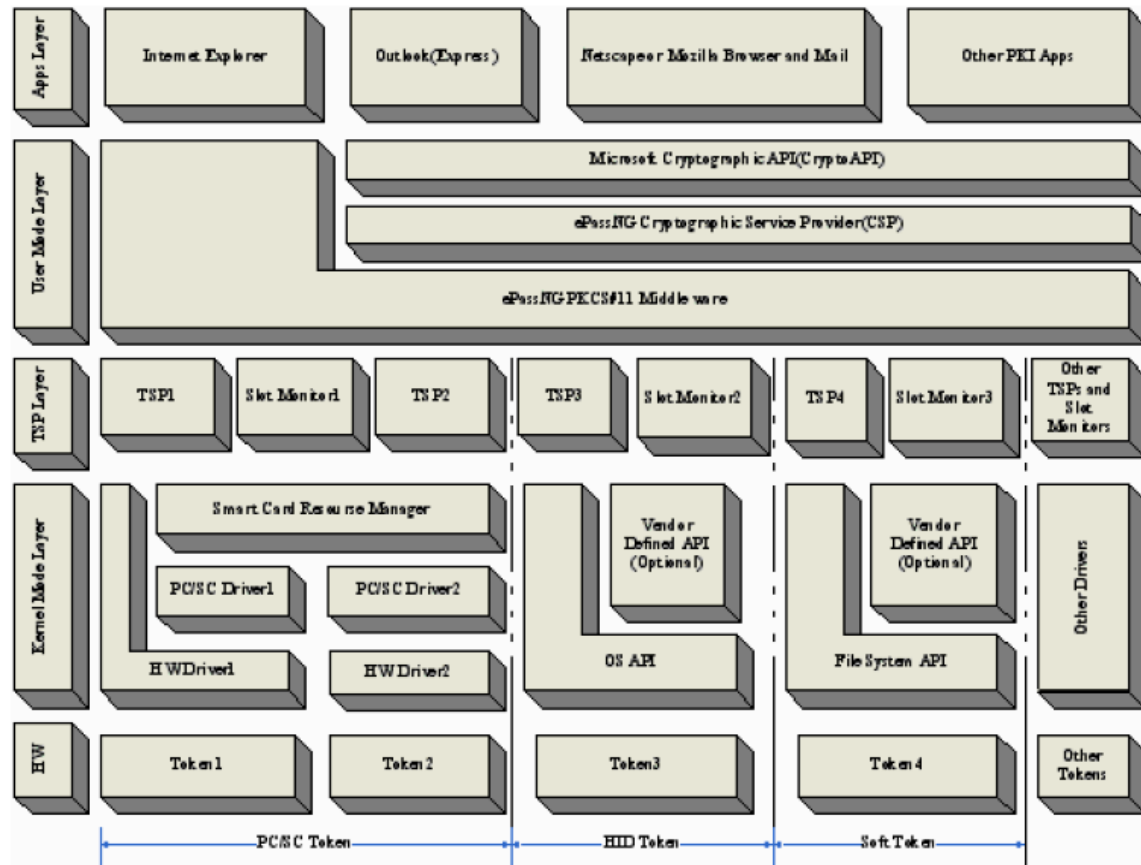
- **Altos Níveis de Segurança:** a função criptográfica on board do dispositivo, baseada no algoritmo RSA, é muito mais segura que uma solução baseada em software. Toda informação sensível permanece armazenada na memória protegida do dispositivo. Todas as operações de assinatura e criptografia são realizadas dentro do dispositivo. A chave privada NUNCA deixa a memória segura do dispositivo, o que garante que ela não será copiada por um hacker, por exemplo. A avançada tecnologia de encapsulamento do chip também garante a segurança física dos dados armazenados no módulo criptográfico.
- **Integração Transparente:** são oferecidos dois padrões industriais reconhecidos: PKCS#11 e Microsoft Crypto API. O Token USB pode ser integrado com qualquer aplicação com qualquer um destes padrões. Além disso, este dispositivo é otimizado para trabalhar com soluções de software de terceiros. Em adição, o Protoken NG possui memória segura para armazenar simultaneamente certificados digitais, chaves privadas, senhas e outras credenciais pessoais, ou seja, suporte a múltiplas aplicações PKI.
- **Alta confiabilidade:** o Protoken NG pode armazenar de forma segura credenciais por pelo menos 10 anos.

5.4 Recursos do Hardware

- **Criptografia:** o dispositivo suporta os seguintes algoritmos: RSA 1024 bits (assinatura e verificação), DES e 3DES; SHA-1 e MD5.
- **Geração do par de chaves:** o par de chaves RSA 1024bits ou 2048bits é gerado no próprio dispositivo.
- **Gerador de números aleatórios:** o dispositivo faz uso de um gerador de números aleatórios real para criar o par de chaves e o MAC (Message Authentication Code).
- **Acesso multi-nível:** existem 16 níveis de acesso do sistema de arquivos do Protoken NG. O sistema de arquivos permite que usuários definam um ou mais privilégios de segurança para o gerenciamento de chave.

5.5 Arquitetura (requisito FIPS 140-2, item 4.1)

É oferecida uma API padrão PC/SC. Desenvolvedores podem fazer uso da função padrão Microsoft Win32 PC/SC para manipular o Token USB Protoken NG.



A arquitetura do sistema consiste em quatro camadas a saber: Hardware, Kernel Driver, Interface do Usuário e Aplicação.

Camada Hardware: consiste no circuito do dispositivo, programa firmware e cabo de conexão. Ele troca dados com o computador via protocolo de comunicação USB da porta USB.

Camada Kernel Driver: manipula a interação de dados entre o PC e a Camada de Hardware, e o acesso ao Token requer a camada de aplicação superior. É a interface do driver PC/SC padrão. As camadas de aplicação superiores podem acessar o Token Protoken NG através do conjunto de funções padrão Win32 PC/SC

Camada Interface do Usuário: as interfaces nesta camada são a PKCS#11 API e a Microsoft CryptoAPI. Elas são suportadas por interfaces inferiores, compatíveis com as aplicações existentes e podem ser desenvolvidas novamente. Por exemplo, algumas aplicações requerem que os usuários assinem digitalmente o conteúdo que eles submetem pelo navegador com o Token Protoken NG. Funções como esta requerem a camada de interface superior.

Camada Aplicação: programas na camada de aplicação incluem geralmente aplicações disponíveis. As interfaces fornecidas pela Feitian são baseadas nos padrões da indústria e são conhecidos da maioria dos desenvolvedores. Os desenvolvedores devem integrar suas aplicações com o Token Protoken NG usando as interfaces fornecidas.

6. Instalando o software do Token USB Protoken NG

6.1 Instalação nos sistemas operacionais Windows 2000, Windows XP, Windows Vista e Windows 2003

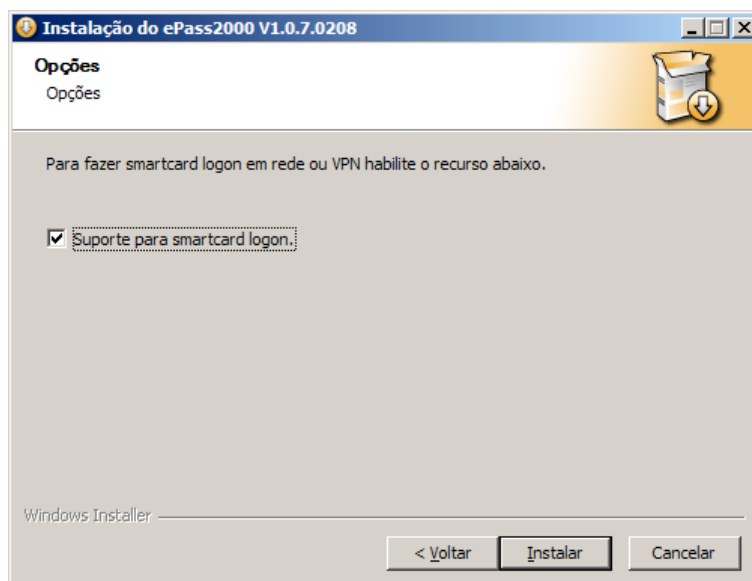
Para instalar o software do Protoken NG, basta inserir CD-ROM fornecido, aguardar a execução do Instalador e seguir as instruções abaixo detalhadas. Se você não possui o CD-ROM, entre em contato com a Pronova Soluções Inteligentes e solicite o instalador.

Nota: se sua unidade de CD-ROM estiver com a função execução automática desabilitada, certamente será necessário executar de forma manual o arquivo runtime.exe.

a) Clique no botão “Avançar” da janela de boas vindas

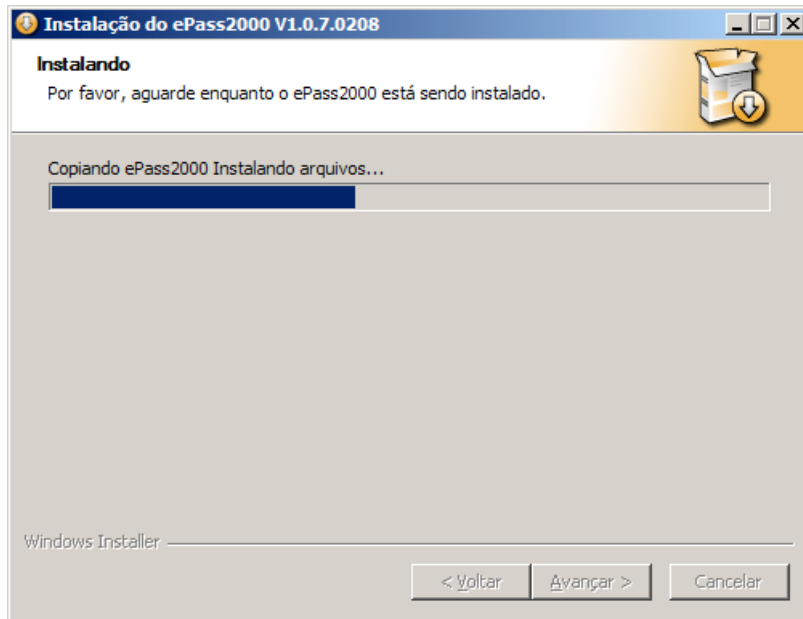


b) Se for fazer login em rede ou VPN usando o Token como um cartão inteligente, habilite a opção “Suporte para sistema de smartcard login em rede ou VPN”. Caso contrário não habilite esta opção. Para continuar clique no botão “Instalar”.

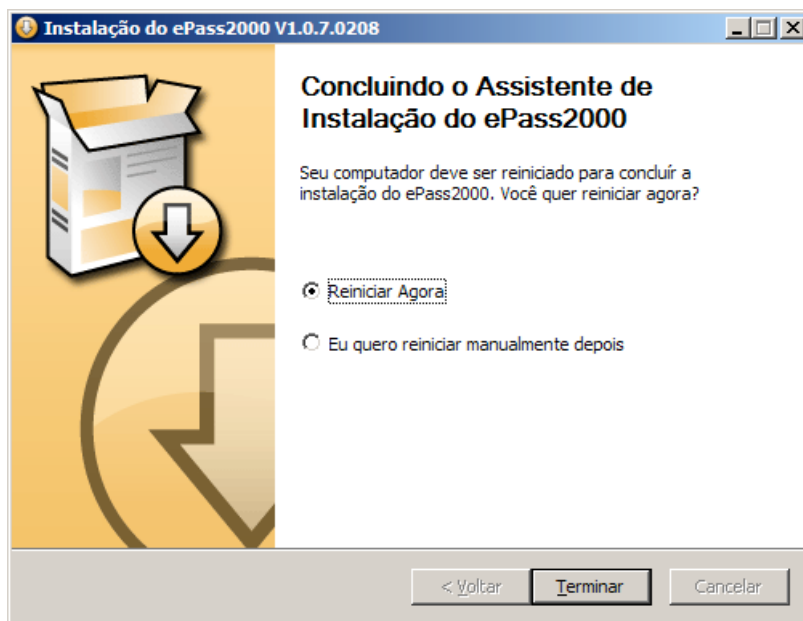


· Para fazer smartcard login é necessário ter um certificado digital para esta finalidade. Ressaltamos ainda que esta funcionalidade somente é suportada nos sistemas operacionais Windows 2000, XP, Vista e 2003. Com relação a VPN, para esta integração ocorrer é necessário que o cliente de VPN da sua solução de firewall já esteja instalado e configurado.

- c) Aguarde que o instalador copie para a sua máquina os arquivos necessários para utilizar o Protoken NG;



- d) Clique no botão “Terminar” para concluir a instalação do Runtime e reiniciar o seu computador;



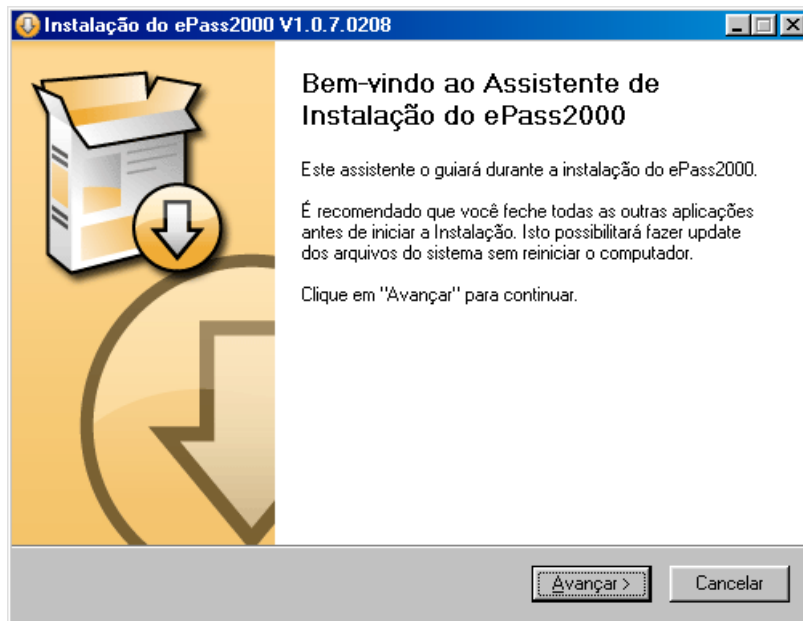
- e) Ao final do novo boot, conecte o seu Protoken NG em uma porta USB livre e aguarde que o sistema operacional reconheça este novo hardware. Durante o processo de reconhecimento do novo hardware o LED (luz) do Protoken NG ficará piscando.

6.2 Instalação nos sistemas operacionais Windows 98SE e Windows ME

Para instalar o software do Protoken NG, basta inserir CD-ROM fornecido, aguardar a execução do Instalador e seguir as instruções abaixo detalhadas. Se você não possui o CD-ROM, entre em contato com a Pronova Soluções Inteligentes e solicite o instalador.

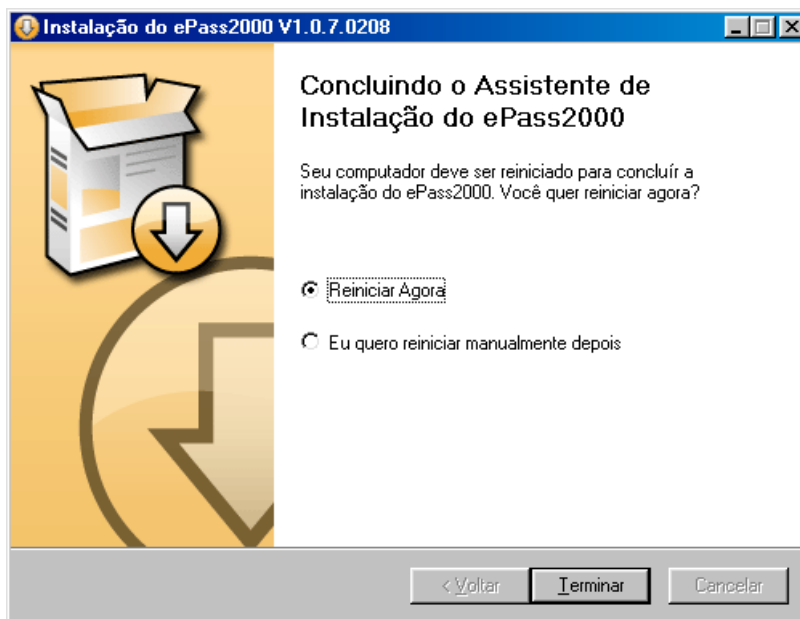
Nota: se sua unidade de CD-ROM estiver com a função autorun desabilitada, certamente será necessário executar de forma manual o arquivo runtime.exe.

a) Clique no botão “Avançar” da janela de boas vindas



b) Aguarde que o instalador copie para a sua máquina os arquivos necessários para utilizar o Protoken NG, bem como o sistema operacional reconheça os novos recursos que estão sendo instalados;

c) Clique no botão “Terminar” para concluir a instalação do Runtime e reiniciar o seu computador.



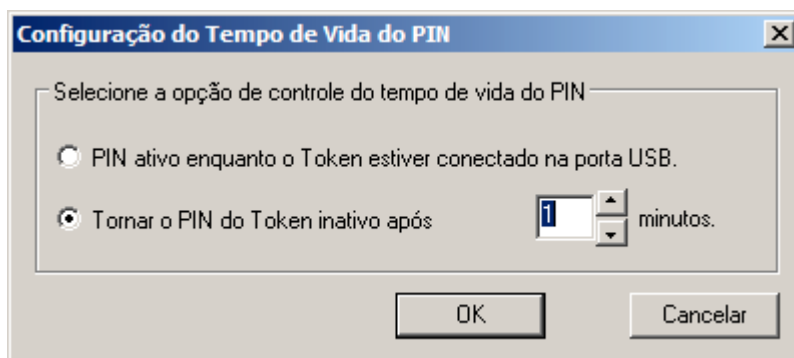
6.3 Configurando o Tempo de Vida do PIN do Protoken NG

Você poderá definir o tempo de vida do PIN do seu Protoken NG. Este recurso pode ser configurado a partir do ícone do Monitor de Certificados que está localizado na área de notificação do Windows. Para dar início a configuração, com o seu dispositivo conectado em uma porta USB, dê dois cliques no ícone do Monitor de Certificados do Protoken NG.

Na janela do Monitor de Certificados do Protoken NG, dê um clique no botão “PIN Timeout”



Na janela “Configuração do Tempo de Vida do PIN”, selecione a opção “Tornar o PIN do Token inativo após” e no campo a seguir digite o valor em minutos desejado. Para concluir esta operação, clique no botão “OK”.



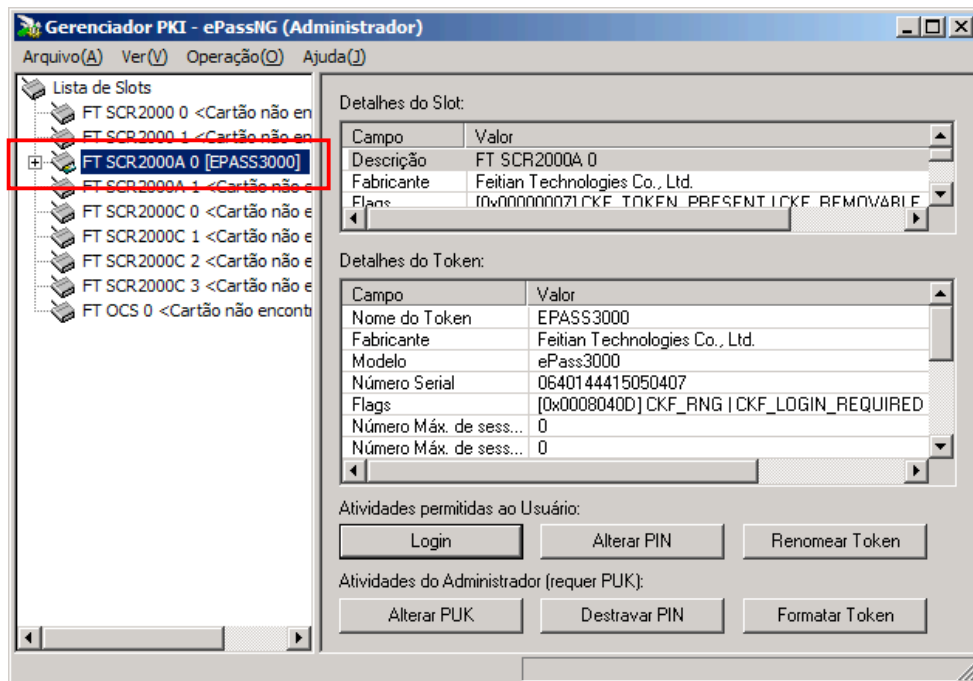
7. O que é o PUK (PIN unlock key) – (item 2.1.b do DOC-ICP-10.03)

O PUK (PIN Unlock Key) é a senha máster que permite ao usuário recuperar o PIN do Usuário e, também formatar o setor PKI do Protoken NG. O valor de fábrica é “12345678” (sem as aspas). Por questões de segurança, este PIN Unlock Key possui um número máximo de tentativas de acerto. *Tenha cuidado para não exceder as 5 (cinco) tentativas*, pois se o PUK for travado, será necessário reformatar o Protoken NG com uma ferramenta específica, a qual irá apagar todo o conteúdo que estiver armazenado no seu Protoken NG.

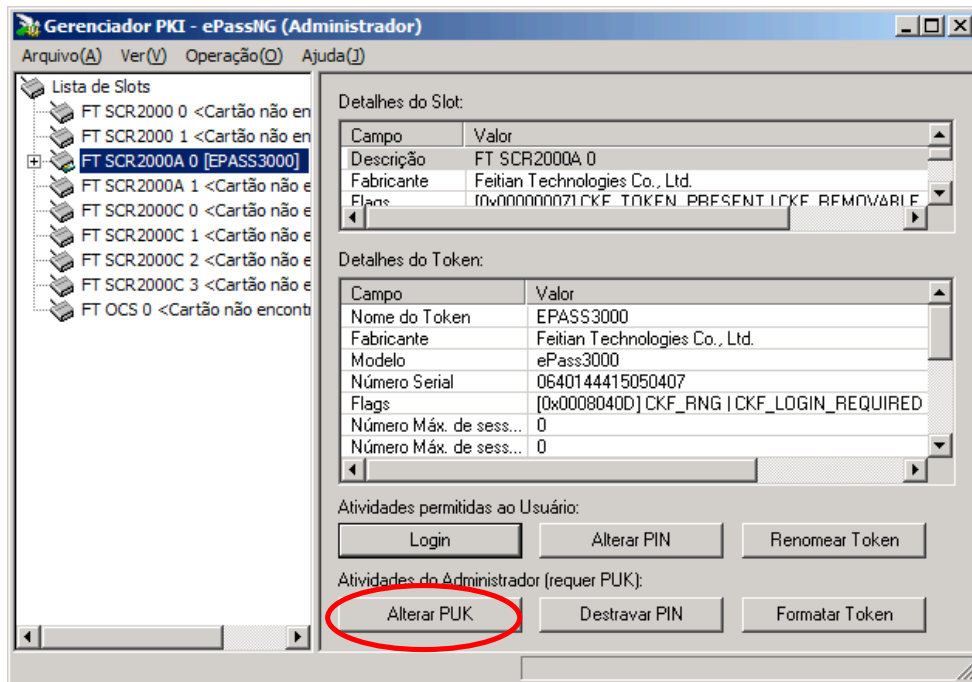
Por questões de segurança e de privacidade, recomendamos que o PUK seja alterado assim que seja possível, ou seja, na primeira utilização. Depois que esta alteração for realizada, o PUK deverá ser guardado em um local seguro. Esta senha máster deve ter no mínimo 8 (oito) caracteres.

7.1 Como alterar o PUK?

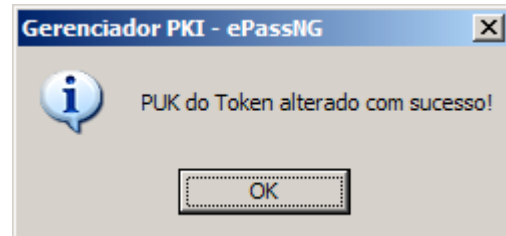
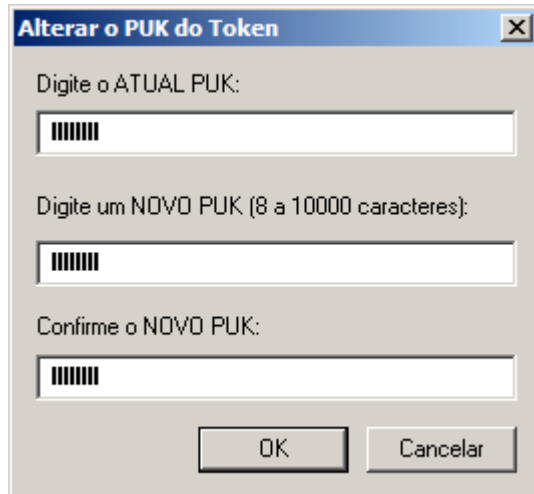
Esta é uma tarefa muito simples. Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR | PROGRAMAS | USB Token | USB Token 3000 | Gerenciador do Token. No Gerenciador, clique no slot referente ao seu Protoken NG.



Clique no botão “Alterar PUK” ter acesso à janela “Alterar PUK”



Se esta for a sua primeira utilização, no campo ‘Digite o ATUAL PUK’, digite 12345678 que é o valor de fábrica do PUK. No campo ‘Digite um NOVO PUK’ digite o valor que você deseja para o seu dispositivo. Confirme este valor no campo ‘Confirme o NOVO PUK’. Para concluir esta operação, clique no botão “OK” e aguarde a exibição da mensagem “PUK do Token alterado com sucesso” (imagem 7.4):



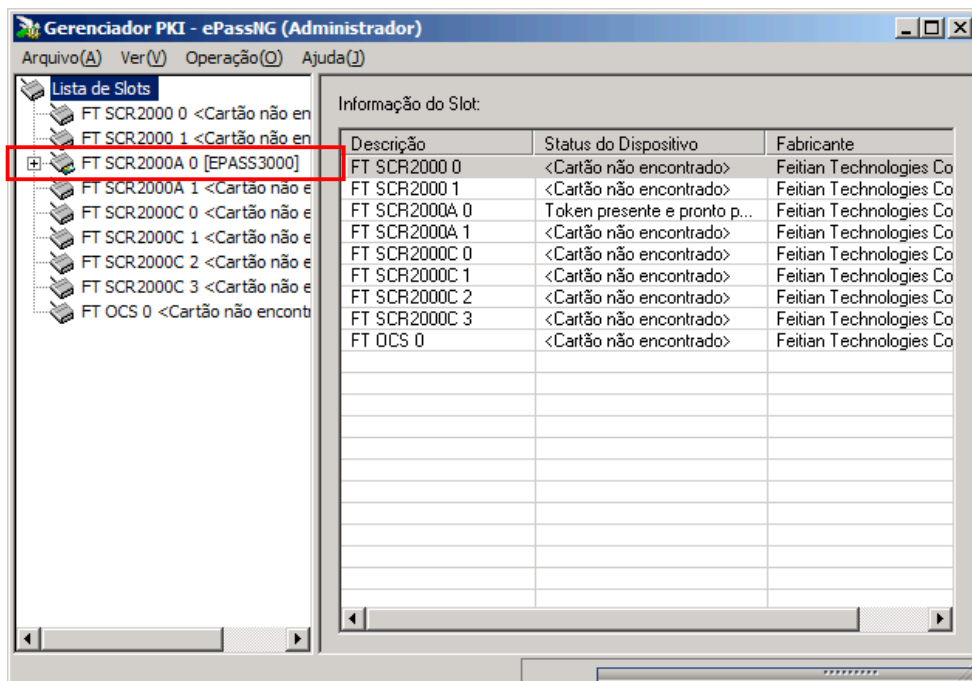
(imagem 7.4)

8. O que é o PIN do Usuário? (requisito FIPS 140-2, item 4.3.1)

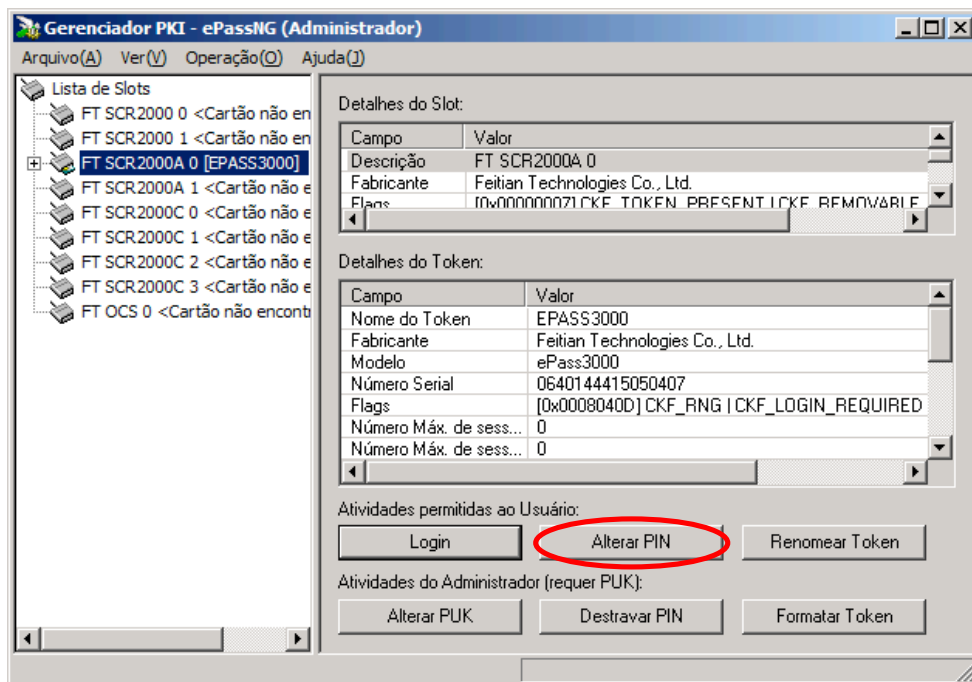
O PIN do Usuário é a senha que será utilizada pelo usuário do dispositivo todas as vezes que for necessário ter acesso às informações pessoais que estão armazenadas no chip criptográfico. O valor de fábrica do PIN do Usuário é "12345678" (sem as aspas) e da mesma forma que o PUK, também existe um número determinado de acertos desta senha, mas neste caso podem ser feitas até 5 (cinco) tentativas consecutivas de acerto desta senha. Ao contrário do PUK, você poderá destravar o PIN do Usuário (mais informações, consulte o tópico 8.1 "Destravando o PIN do Usuário").

Para alterar o PIN do Usuário, siga as instruções a seguir:

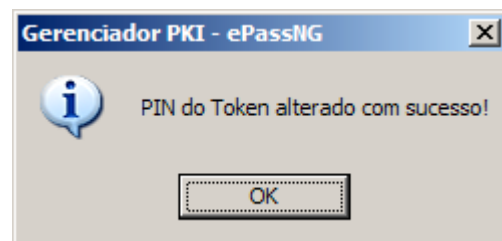
Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR | PROGRAMAS | USB Token | USB Token 3000 | Gerenciador do Token. A seguir, clique no slot referente ao seu Protoken NG para que as opções de operação sejam exibidas



Clique no botão 'Alterar PIN' para ter acesso a janela 'Alterar PIN'.



Se você estiver usando seu Protoken NG pela primeira vez, certamente ele ainda deverá estar com o PIN de fábrica que é "12345678" (sem as aspas). Neste caso, no campo 'Digite o ATUAL PIN', digite 12345678 e nos campos 'Digite um NOVO PIN' e 'Confirme o NOVO PIN' digite o PIN mais apropriado para você. Por questões de segurança, recomendamos que este PIN tenha no mínimo 8 caracteres e que seja composto de letras e números. Depois de preencher todos os campos clique no botão OK e aguarde que a mensagem 'PIN alterado com sucesso!' seja exibida (imagem 8.4).

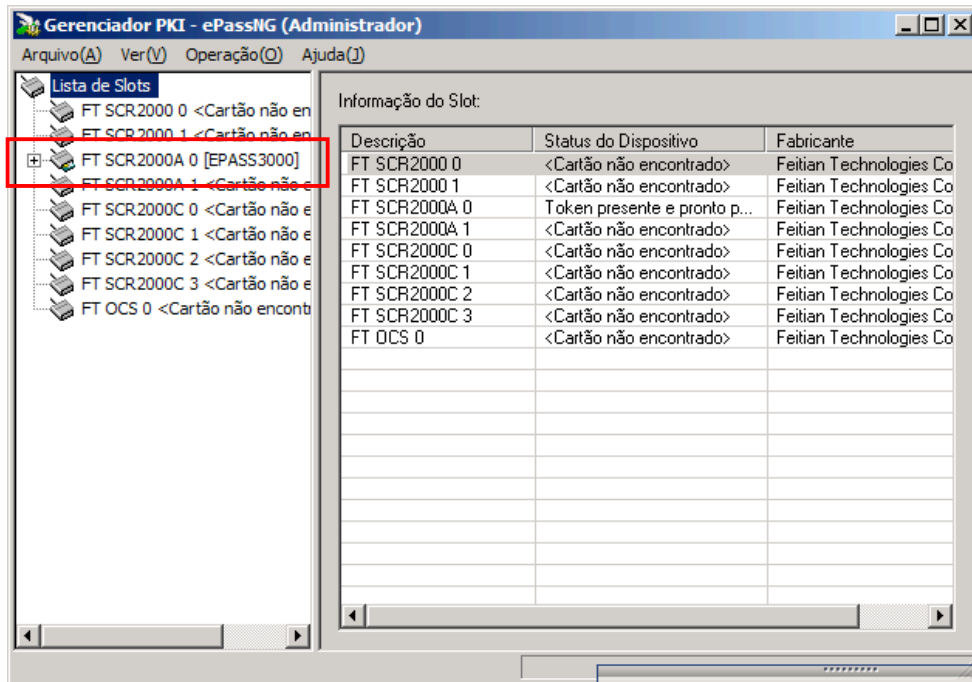


(imagem 8.4)

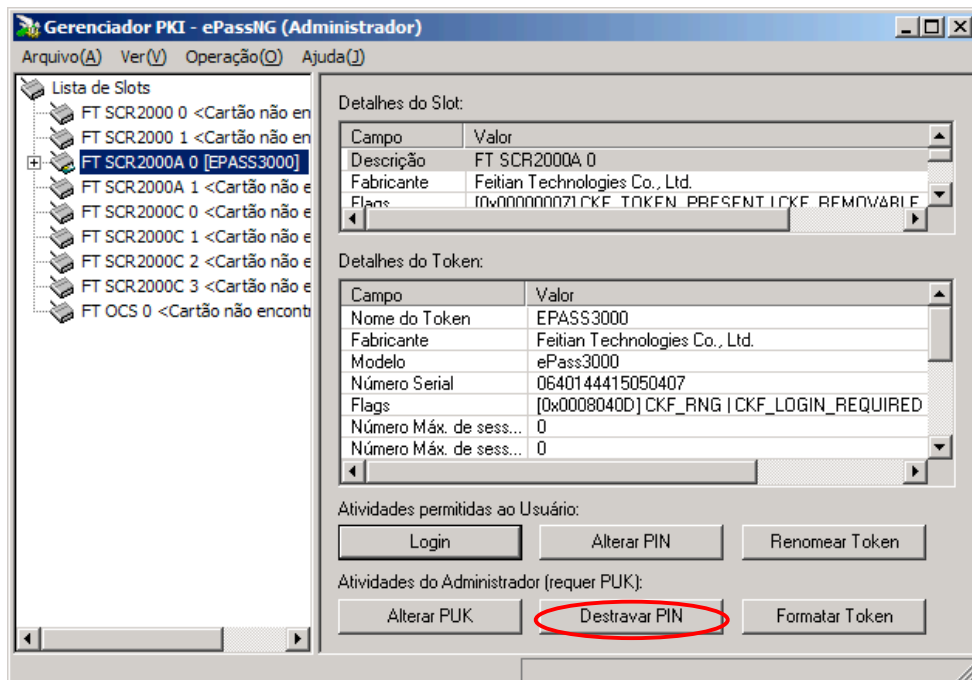
8.1 Destravando o PIN do Usuário

Para destravar o PIN do Usuário, siga as instruções a seguir:

Com o seu dispositivo conectado, execute o *Gerenciador* a partir do atalho criado em INICIAR | PROGRAMAS | USB Token | USB Token 3000 | Gerenciador do Token. Clique no slot referente ao seu Protoken NG para que as opções de operação sejam exibidas.

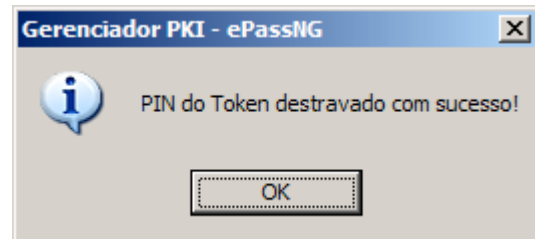


Clique no botão 'Destravar PIN' para ter acesso a janela 'Destravar PIN do Usuário'



ATENÇÃO: antes de iniciar este procedimento tenha absoluta certeza de que está de posse do PUK do dispositivo! Se ocorrer cinco tentativas de acesso com o PUK incorreto, o seu Token será totalmente travado e será necessário re-formatar o seu Protoken NG, perdendo assim todas as informações que estão armazenadas no equipamento.

No campo 'Digite o PUK do Token', digite o PUK do seu dispositivo. Nos campos 'Digite um NOVO PIN' e 'Confirme o NOVO PIN' digite um novo PIN para o seu Protoken NG. Após preencher todos os campos, clique no botão OK e aguarde que a mensagem 'PIN do Token destravado com sucesso!' (imagem 8.1.4).

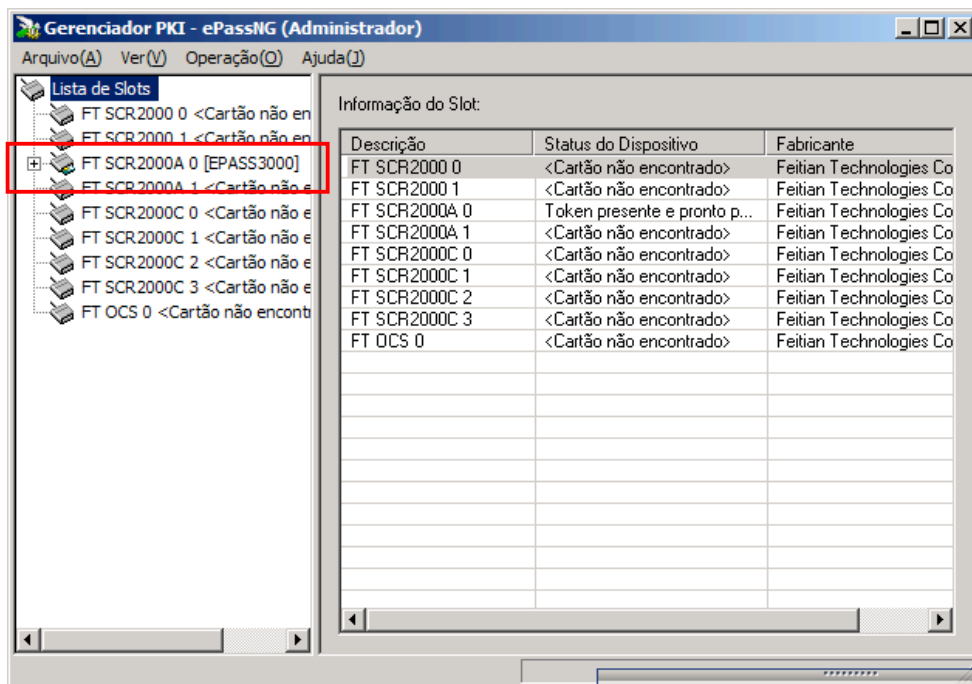


(imagem 8.1.4)

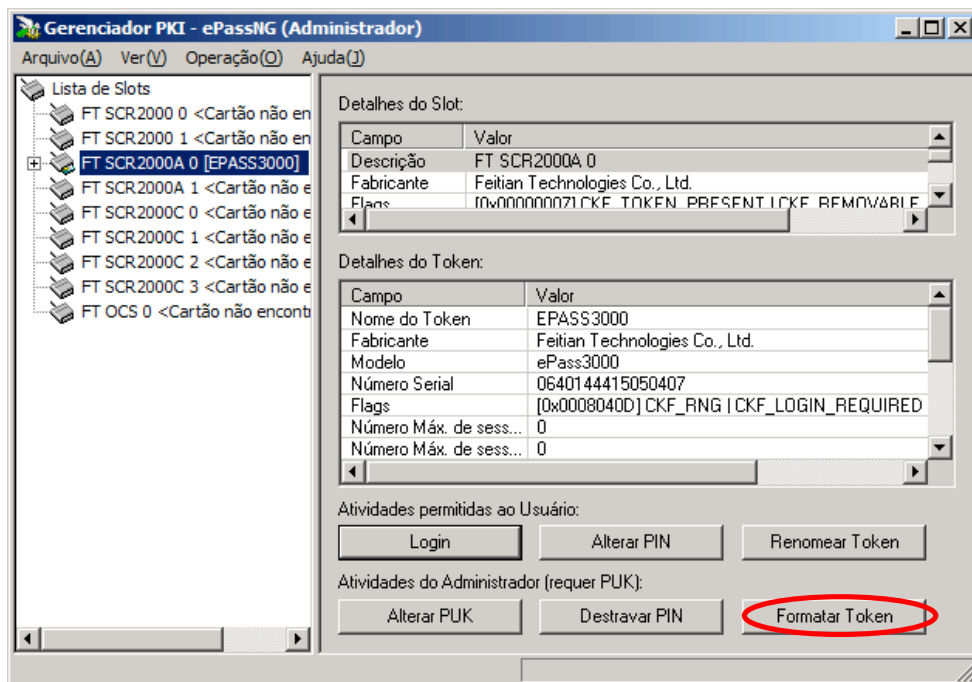
9. Formatando o Setor PKI do Protoken NG

Sempre que você julgar necessário apagar todo o conteúdo (certificados e chaves criptográficas) do Protoken NG, faça uso do recurso “Formatar Token” do Gerenciador. Para tal, execute-o a partir do atalho criado no Grupo ePassNG que pode ser acessado a partir do botão “Iniciar do Windows. Clique no slot referente ao seu Protoken NG para que as opções de operação sejam exibidas

ATENÇÃO: esta é uma ação irreversível e que vai apagar todas as informações que estiverem armazenadas no Protoken NG.



Clique no botão 'Formatar Token' para ter acesso a janela 'Formatar o Token (Inicializar Setor PKI)'.



No campo 'Digite o ATUAL PUK do Token' digite o PUK. Nos campos 'Digite um NOVO PIN' e 'Confirme o NOVO PIN', digite um novo PIN para o seu Protoken NG. Se desejar que o seu dispositivo tenha um nome específico, digite o nome desejado no campo 'Digite um nome para o Token'. Depois de preencher todos os campos, clique no botão "OK". Uma janela (imagem 9.4) informando que o processo vai apagar todas as informações do Token será exibida. Se você estiver certo de que deseja apagar TODOS os dados que estão armazenados no equipamento, clique no botão 'Sim' para continuar. Do contrário, clique no botão 'Não' para cancelar a operação.

Formatar o Token (Inicializar Setor PKI)

Digite o ATUAL PUK do Token:

██████

Digite um NOVO PIN (8 a 10000 caracteres):

██████

Confirme o NOVO PIN do Token:

██████

Digite um nome para o Token (máx. 32 caract.):

MAURICIO

OK Cancelar

ePassNG PKI Manager

? O processo de formatação vai apagar todas as informações do Token, deseja continuar?

Sim Não

(imagem 9.4)

Se você clicou no botão 'Sim' a mensagem "Token formatado com sucesso! Todas as informações que estavam armazenadas no Token foram apagadas" será exibida (imagem 9.5).

Gerenciador PKI - ePassNG

i Token formatado com sucesso!
Todas as informações que estavam armazenadas no Token foram apagadas!

OK

(imagem 9.5)

10. Instalando um certificado emitido por uma AC Microsoft no Protoken NG

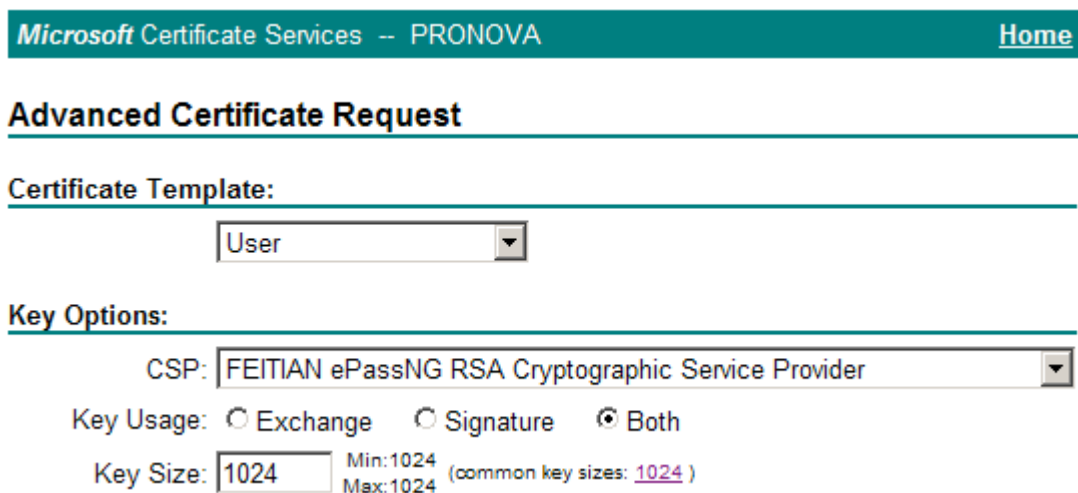
ATENÇÃO: você apenas poderá executar os passos descritos neste tópico se você ou sua empresa possuir um servidor Windows 2000 ou Windows 2003 com o serviço Autoridade Certificadora (Certificate Authority) instalado e configurado. Se você não possui esta estrutura instalada em sua rede, procure uma Autoridade Certificadora credenciada à ICP-Brasil. Maiores informações sobre as ACs credenciadas à ICP-Brasil, consulte www.iti.gov.br.

Instalar um certificado digital no Protoken NG é uma tarefa muito simples. Entretanto, é importante ressaltar que o processo deverá ser concluído na mesma máquina onde o processo de solicitação foi iniciado.

Você poderá instalar qualquer certificado digital cujo par de chaves seja de até 1024bits, inclusive ICP-Brasil (desde que solicitado a partir de uma AC credenciada a ICP-Brasil), mas é necessário aqui estar atento à capacidade de armazenamento do seu dispositivo, ou seja, a quantidade de certificados armazenados vai variar do tamanho destes e da memória de 64K do seu Protoken NG. Com o seu dispositivo conectado em uma porta USB, acesse a página web onde será feita a solicitação do certificado digital.

Nosso exemplo fará uso da Autoridade Certificadora PRONOVA que roda em uma plataforma Microsoft. Não registraremos aqui neste guia as telas iniciais onde o usuário informa o nome, o e-mail, telefone e demais dados cadastrais.

Apresentaremos o processo a partir da tela onde o usuário terá que selecionar o CSP (Cryptographic Solution Provider) do dispositivo. Na imagem abaixo, note que estamos selecionando a opção “**FEITIAN ePassNG RSA Cryptographic Service Provider**”.



Microsoft Certificate Services -- PRONOVA [Home](#)

Advanced Certificate Request

Certificate Template:

User

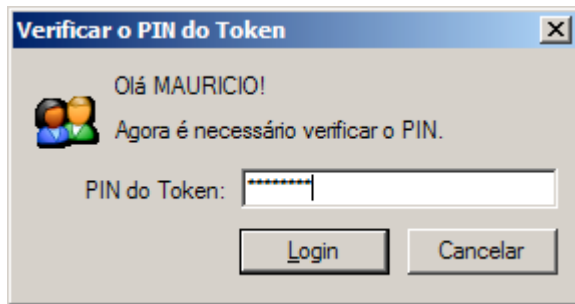
Key Options:

CSP: FEITIAN ePassNG RSA Cryptographic Service Provider

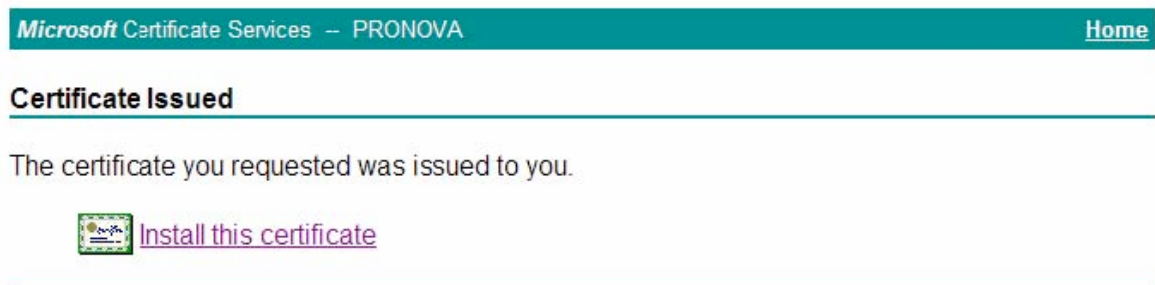
Key Usage: ☐ Exchange ☐ Signature ☒ Both

Key Size: 1024 Min: 1024 Max: 1024 (common key sizes: 1024)

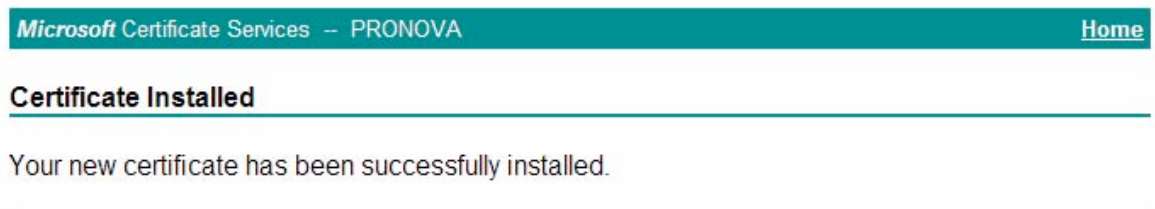
Ao clicar no botão “Submit” da página de solicitação do certificado digital, uma tela solicitando o PIN do Usuário irá surgir. Informe o PIN e clique no botão “Login”.



Se o PIN informado for o correto, observe as mensagens que serão exibidas na área de notificação do Windows. Ao informar PIN correto o par de chaves será gerado dentro do seu Protoken NG e ao término deste processo o usuário é encaminhado para a próxima página.



Para concluir a instalação, clique no link “Install this certificate” e a próxima página será exibida.

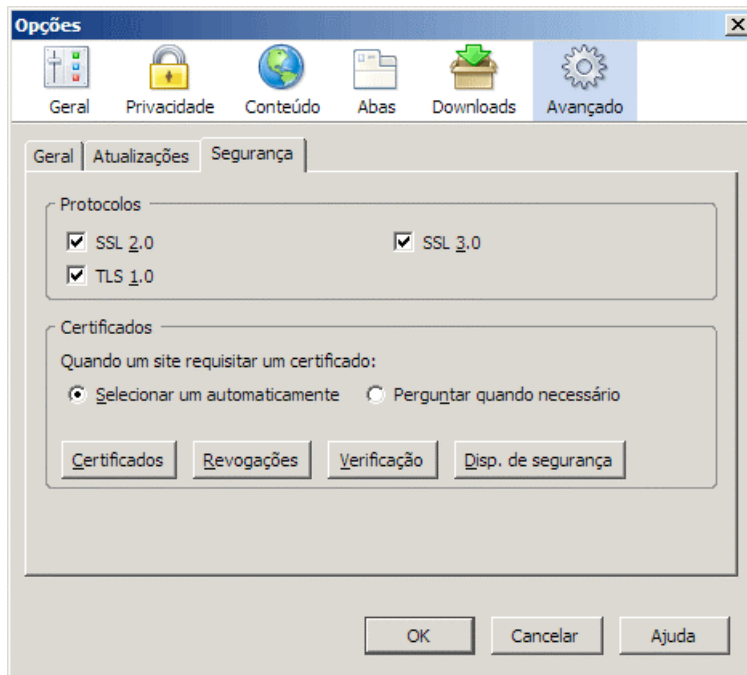


Pronto, seu certificado já está armazenado no Protoken NG!

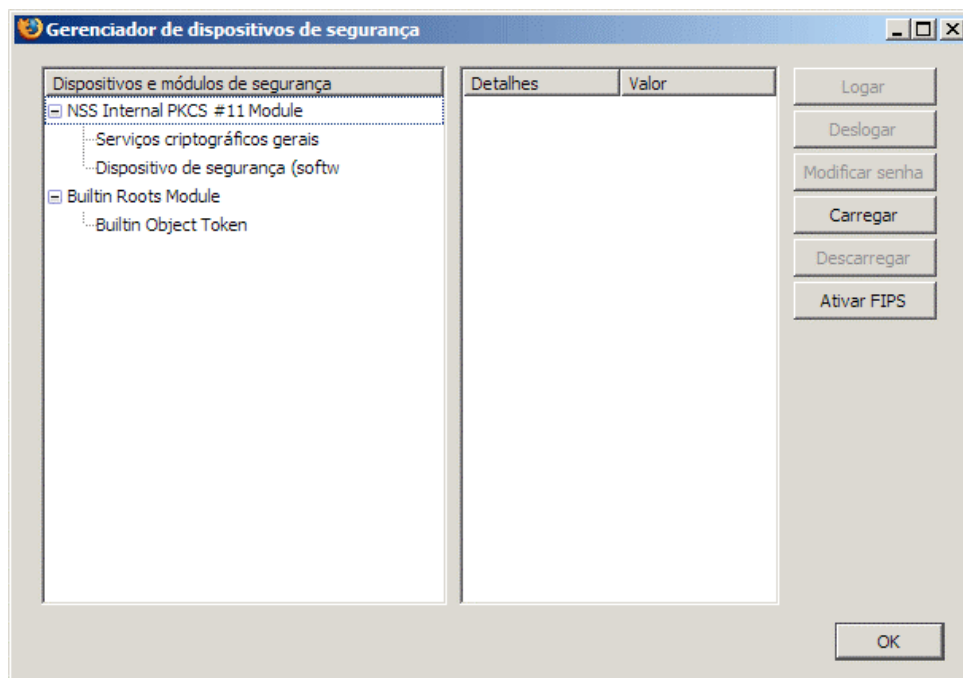
11. Integrando o Protoken NG com o Mozilla Firefox 1.5

ATENÇÃO: siga apenas estes procedimentos, caso o instalador do software do Protoken NG seja anterior a versão 1.0.8.709 que foi liberada em 25/07/2008. Fora isso, os procedimentos abaixo mencionados não precisam ser realizados com o Internet Explorer!!!

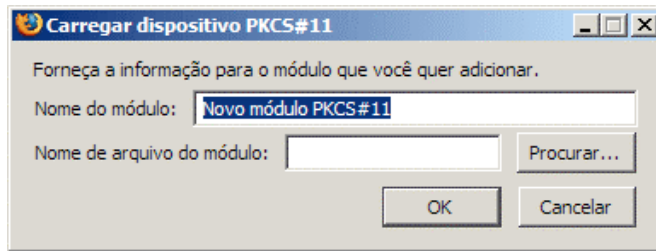
1. Clique em “Ferramentas” da barra de menu e depois em “Opções...”
2. Na janela “Opções”, clique na opção “Avançado” e depois no botão “Disp. De segurança”



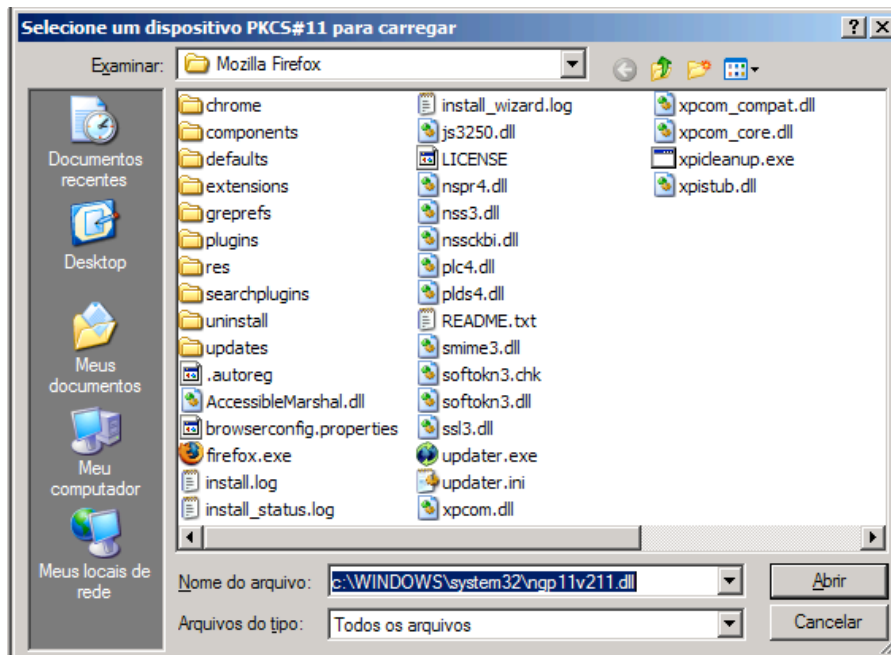
3. Na janela “Gerenciador de dispositivos de segurança”, clique no botão “Carregar”



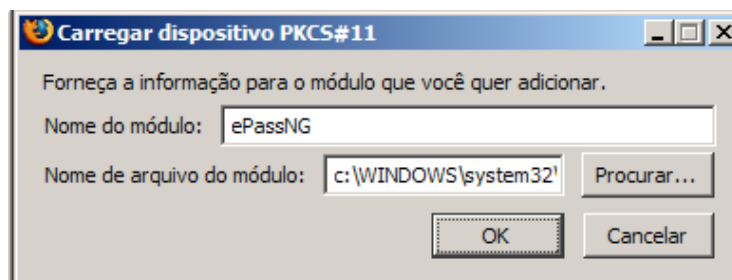
4. Uma janela chamada “Carregar dispositivo PKCS#11” será exibida, clique no botão “Procurar...” desta janela



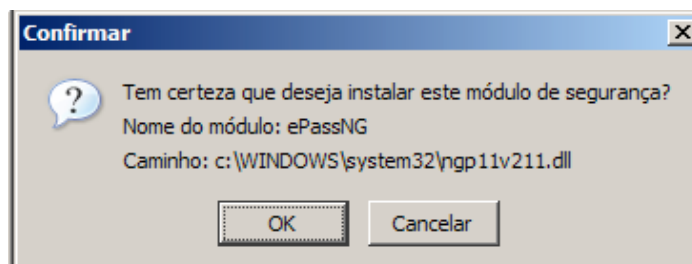
5. Na janela “Selecione um dispositivo PKCS#11 para carregar”, localize o arquivo ngp11v211.dll (este arquivo se encontra no diretório System32 do Windows)



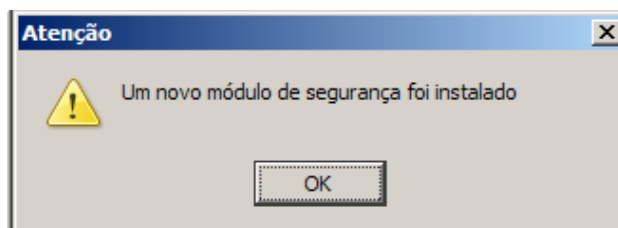
6. De volta a janela “Carregar dispositivo PKCS#11”, no campo “Nome do módulo” digite ePassNG. A seguir clique no botão “OK”



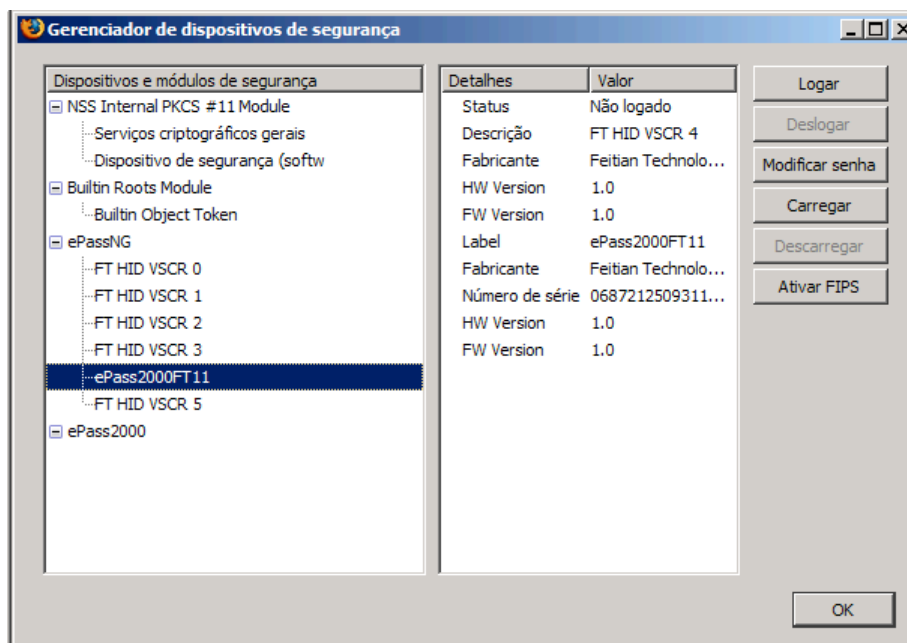
7. Clique no botão “OK” da janela “Confirmar”



8. Clique no botão “OK” da janela “Atenção”



9. Clique no botão “OK” da janela “Gerenciador de dispositivos de segurança”

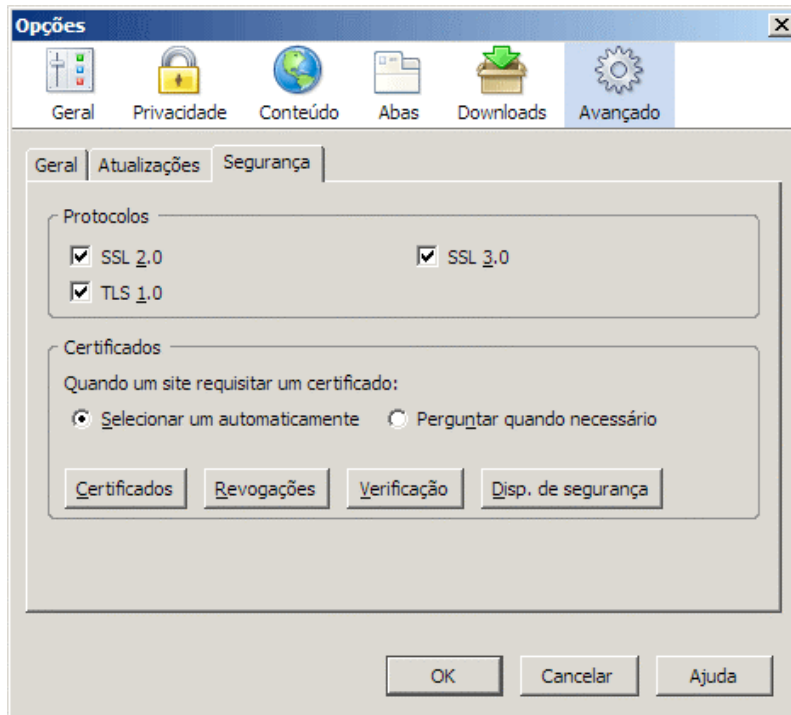


10. Clique no botão “OK” da janela “Opções” para concluir.

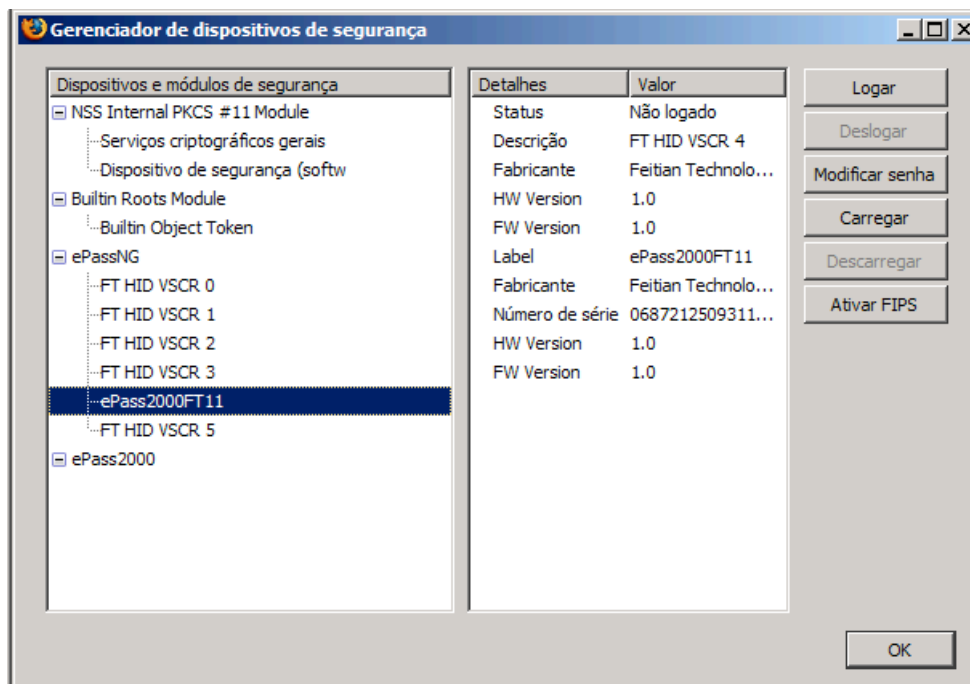
12. Utilizando o Firefox 1.5 para alterar o PIN do Usuário do Protoken NG

a) Clique em “Ferramentas” da barra de menu e depois em “Opções...”

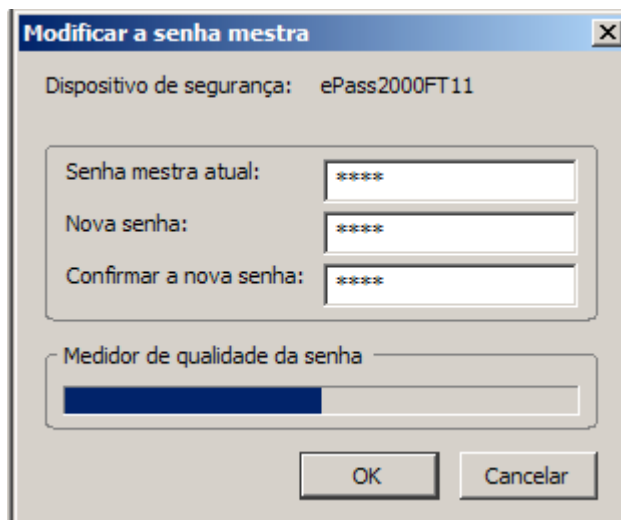
b) Na janela “Opções”, clique na opção “Avançado” e depois no botão “Disp. De segurança”



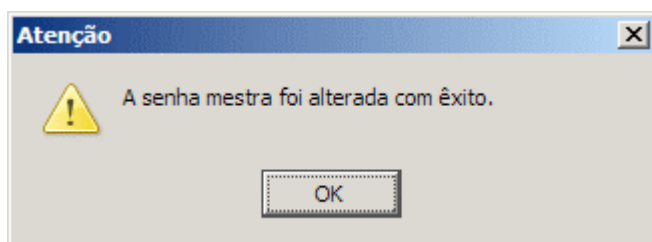
c) Na janela “Gerenciador de dispositivos de segurança”, clique no nome do seu ePassNG e depois no botão “Modificar Senha”



d) Uma janela chamada “Modificar a senha mestra” será exibida. No campo “Senha mestra atual” digite o atual PIN do Usuário, nos campos seguintes digite o novo PIN do Usuário. Ao final, clique no botão “OK” para concluir a operação



e) Assim que a operação for concluída, clique no botão “OK” da janela “Aviso”



f) Clique no botão “OK” da janela “Gerenciador de dispositivos de segurança”

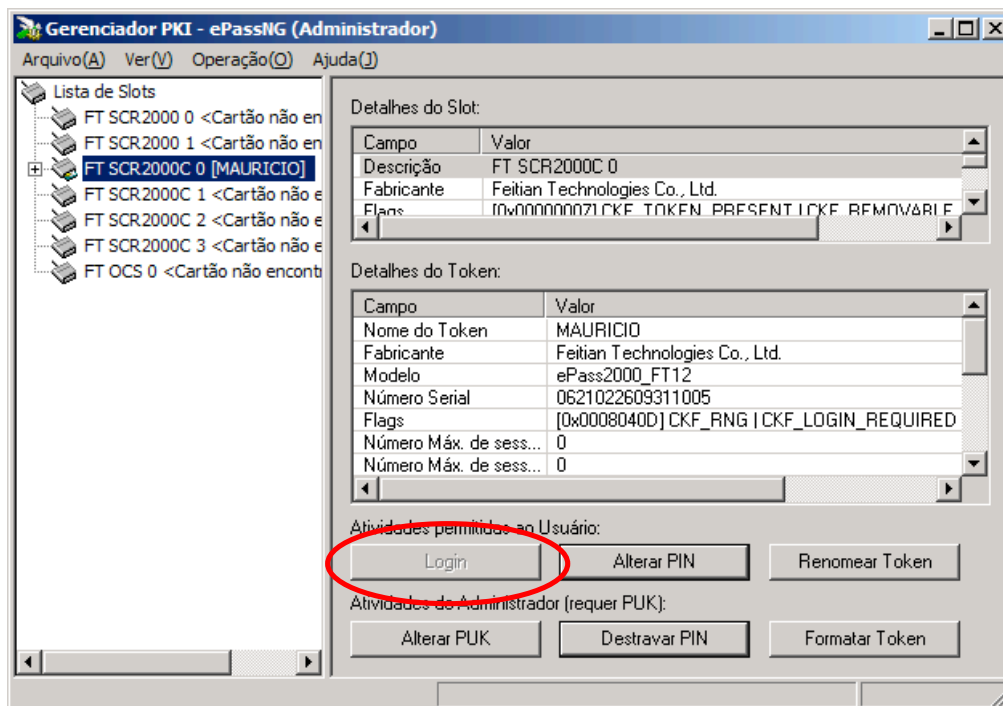
g) Clique no botão “OK” da janela “Opções” para concluir.

13. Importando um certificado para o Protoken NG a partir de um arquivo

NOTA: certificados digitais do tipo A3 não possuem cópia de segurança em arquivo formato .PFX ou .P12, pois de acordo com as normas da ICP-Brasil o par de chaves DEVE ser gerado dentro de um dispositivo criptográfico (Token USB ou Cartão Inteligente), tal norma determina que a chave privada não poderá ser exportada para fora do dispositivo criptográfico, impedindo assim a geração deste tipo de arquivo de backup.

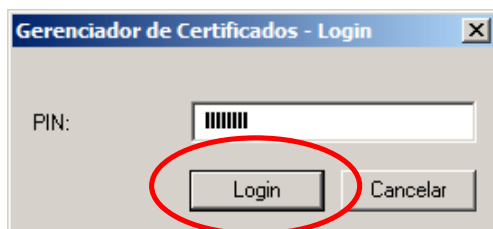
Se você possui uma cópia do seu certificado digital em um arquivo .PFX ou .P12 e deseja importá-lo para o Protoken NG é necessário que você possua a senha do seu arquivo. De posse deste arquivo e da senha do mesmo, siga os seguintes passos:

- Execute o Gerenciador a partir do atalho criado em no grupo INICIAR | PROGRAMAS | ePassNG
- Clique no slot referente ao seu Protoken NG para que as opções de operação sejam exibidas



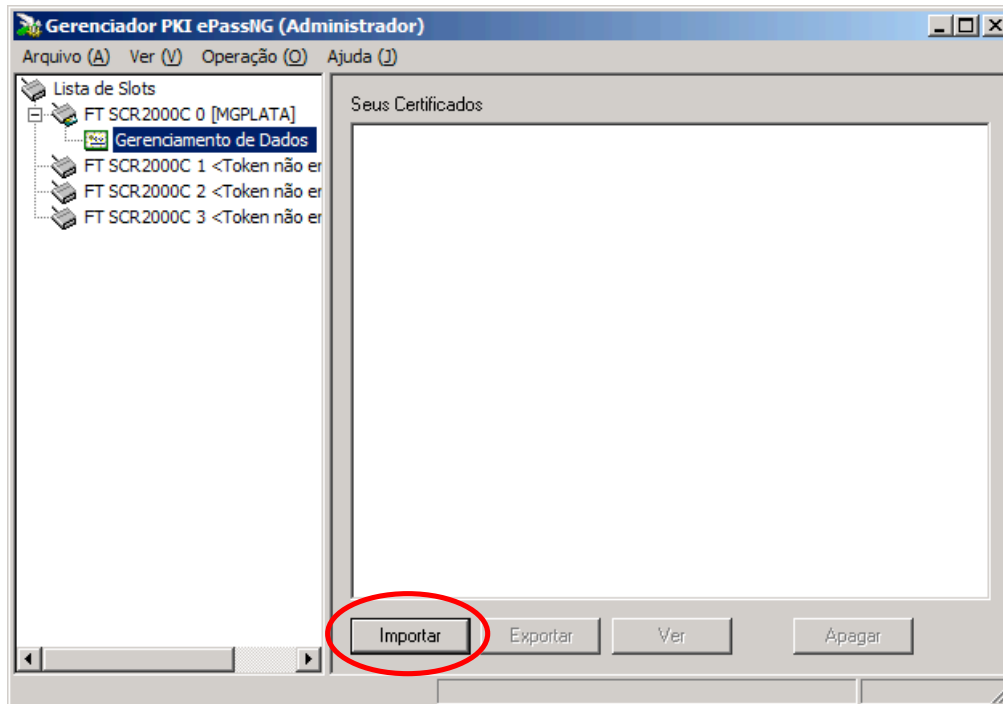
(imagem 13.1)

Clique no botão 'Login' (imagem 13.1) para que a janela 'Gerenciador de Certificados – Login' (imagem 13.2) seja exibida. Nela digite o PIN do seu Token e clique no botão 'Login' para continuar.

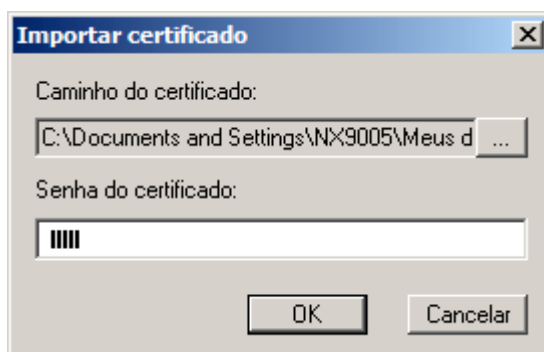
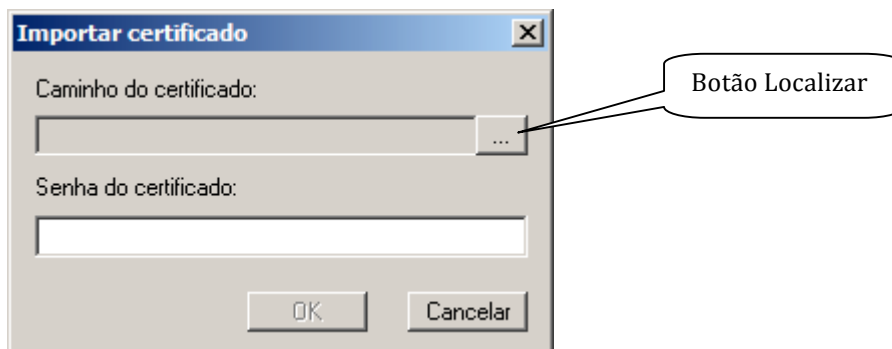


(imagem 13.2)

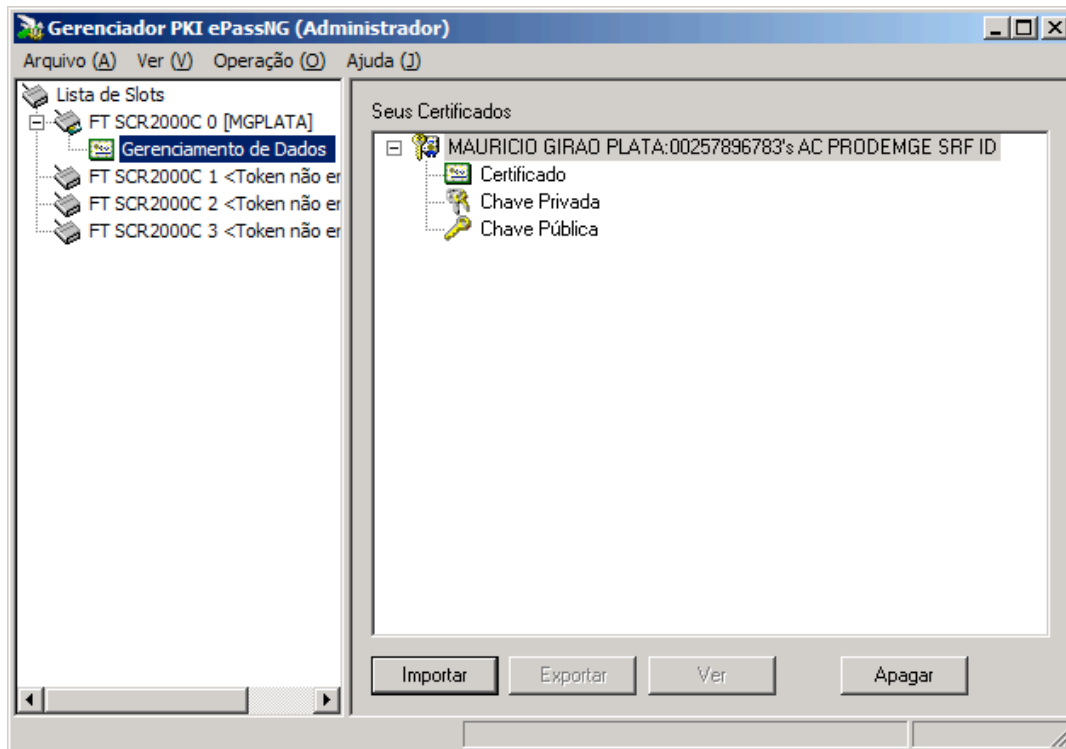
De volta a janela do Gerenciador, você será redirecionado para 'Gerenciamento de dados', para continuar clique no botão 'Importar' para que a janela 'Importar certificado' seja exibida.



Clique no botão 'localizar' para informar o local onde está o arquivo .PFX (ou .P12) e a senha deste arquivo.



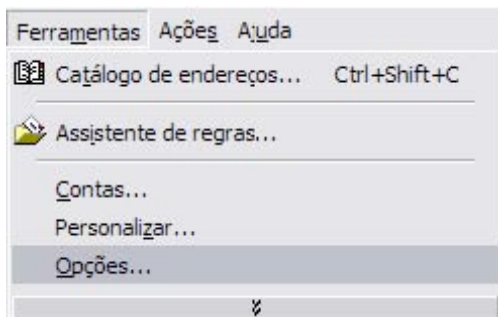
Assim que o certificado for importado para o seu dispositivo, você terá condições de verificar algumas informações do certificado.



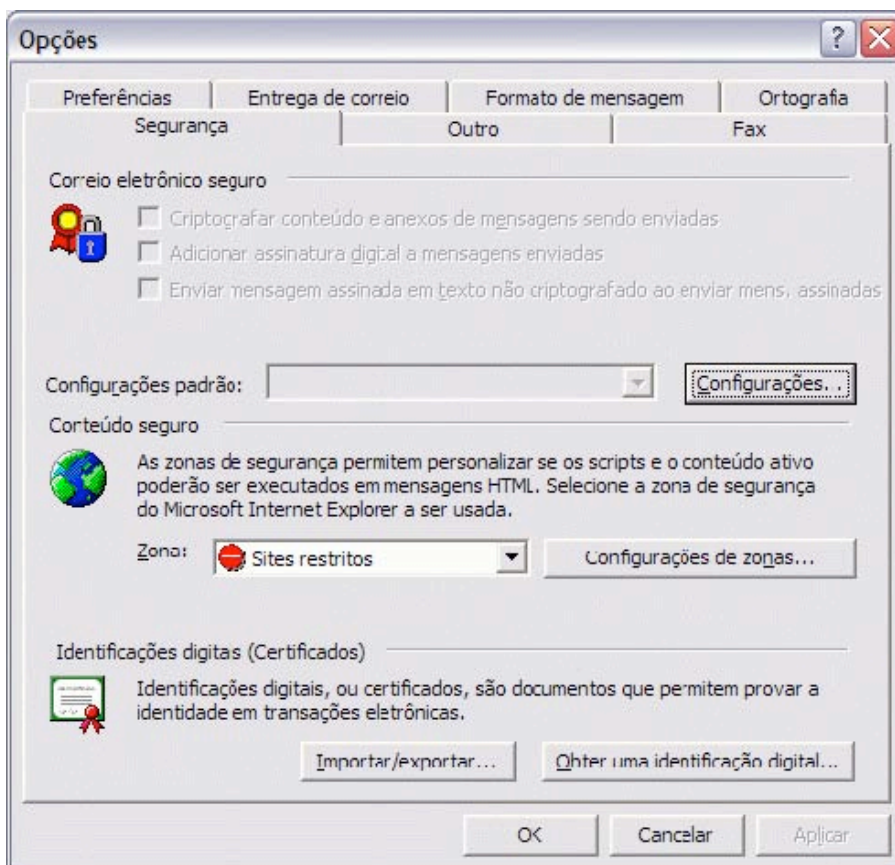
14. Configurando o Microsoft Outlook para usar um certificado armazenado no Protoken NG

Para que as instruções citadas neste capítulo tenham resultado positivo, é necessário observar que o e-mail que está incluso no certificado digital armazenado no Token seja o mesmo da conta do Microsoft Outlook. Siga os passos apresentados neste tópico para que seja possível fazer uso de um certificado digital armazenado no Protoken NG.

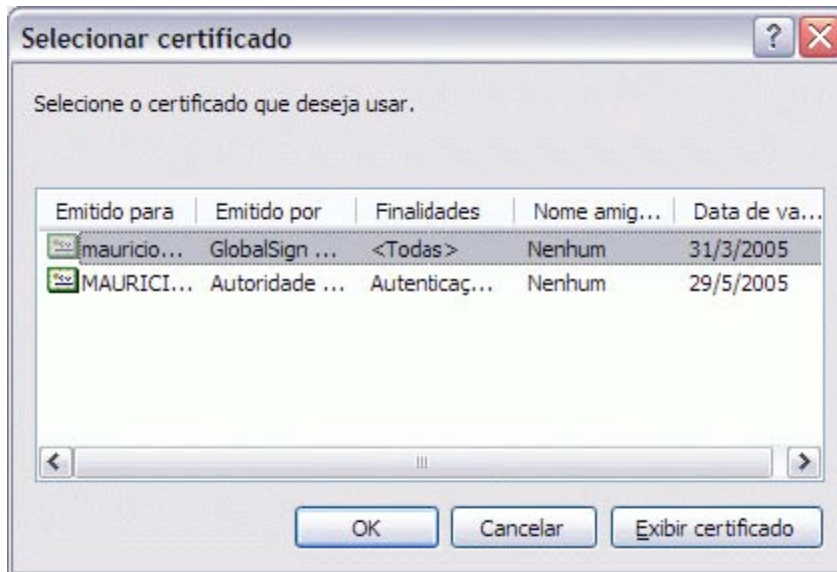
- a) Conecte o seu dispositivo e depois execute o Microsoft Outlook;
- b) Clique em “Ferramentas” da barra de menu e depois em “Opções”;



- c) Na janela “Opções”, clique na guia “Segurança” e depois no botão “Configurações”



- d) Na janela "Alterar configurações de segurança" clique no botão "Escolher" que está à direita do campo "Certificado de Autenticação". Da lista de certificados disponíveis, clique no certificado que corresponde a sua conta de e-mail. Depois no botão "OK";

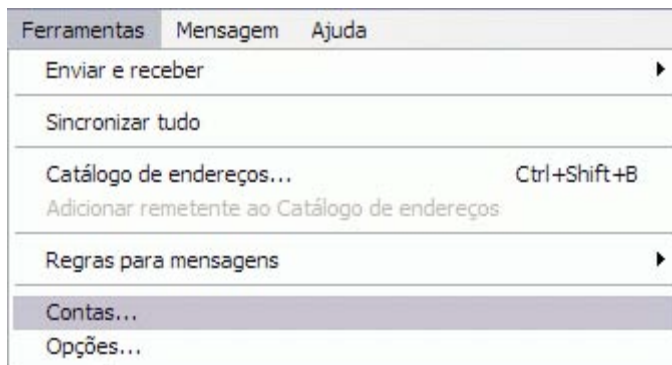


- e) Ainda na janela "Alterar configurações de segurança" clique no botão "Escolher" que está à direita do campo "Certificado de Criptografia". Da lista de certificados disponíveis, clique no certificado que corresponde a sua conta de e-mail. Depois no botão "OK";
- f) Ainda na guia "Segurança", clique na opção "Adicionar assinatura digital a mensagens enviadas". Para concluir clique no botão "OK".
- g) Ao final da seleção a janela "Alterar configurações de segurança" poderá ser fechada. Clique no botão "OK" para continuar.
- h) Na primeira vez que você for enviar uma mensagem assinada, será necessário informar o PIN do Usuário do seu dispositivo.

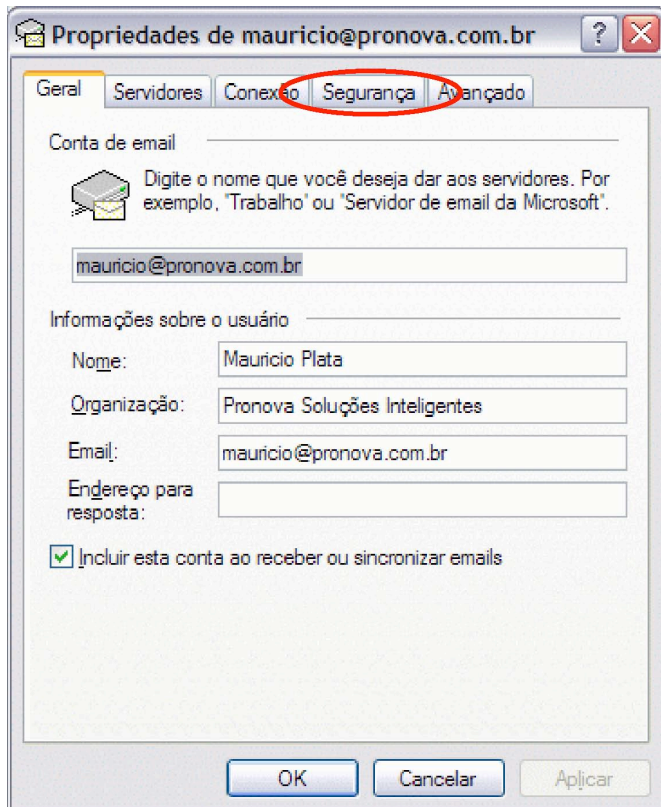
15. Configurando o Outlook Express para usar um certificado armazenado no Protoken NG

Para que as instruções citadas neste capítulo tenham resultado positivo, é necessário observar que o e-mail que está incluso no certificado digital armazenado no Token seja o mesmo da conta do Microsoft Outlook Express. Siga os passos apresentados neste tópico para que seja possível fazer uso de um certificado digital armazenado no seu dispositivo.

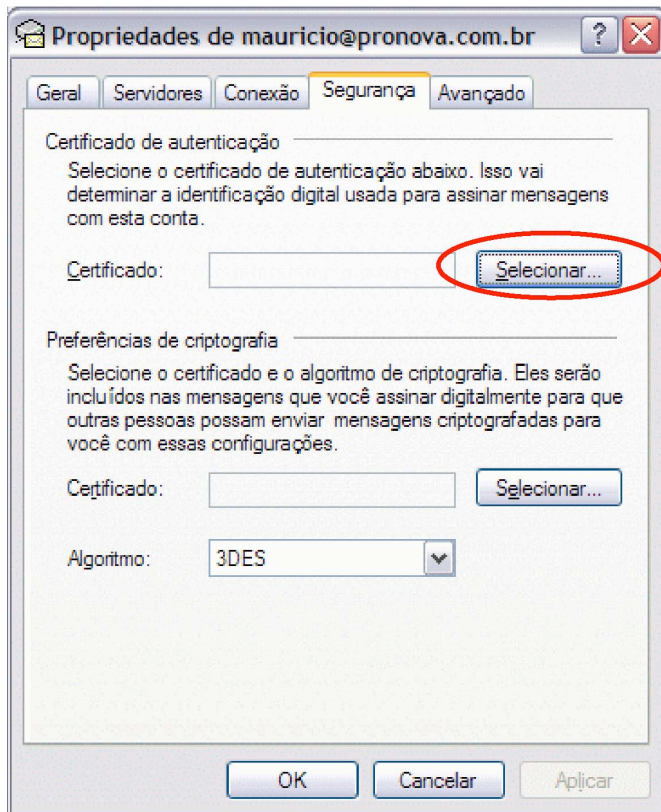
- a) Conecte o seu dispositivo e depois execute o Outlook Express;
- b) Clique em “Ferramentas” da barra de menu e depois em “Contas...”



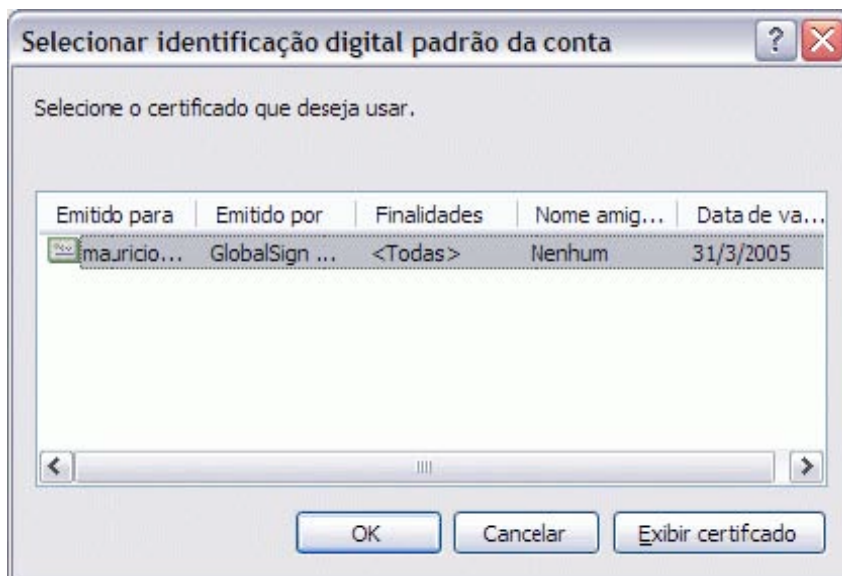
- c) Na janela “Propriedades de...” clique na guia “Segurança”



d) Na guia “Segurança”, clique no botão “Selecionar” que está à direita do campo “Certificado” da área “Certificado de autenticação”

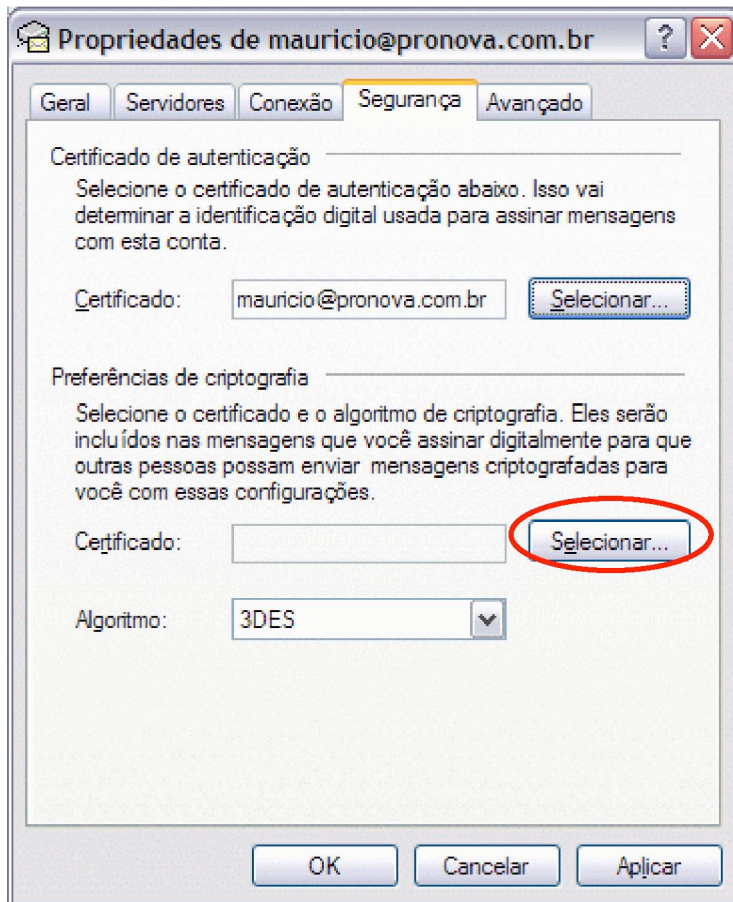


e) Na janela “Selecionar identificação digital padrão da conta”, selecione o certificado digital referente à conta em uso, em seguida clique no botão “OK”.

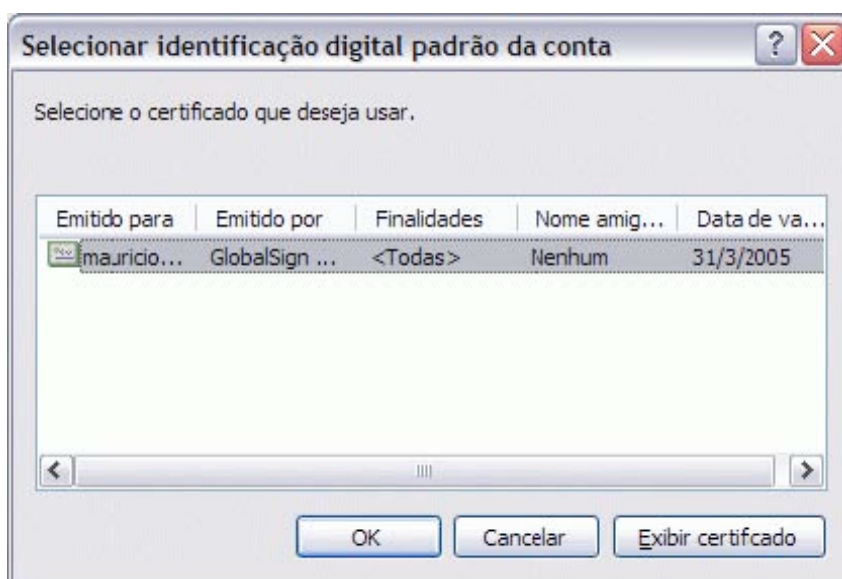


Se você deseja visualizar as informações sobre o certificado digital, clique no botão “Exibir Certificado”

f) De volta a janela “Propriedades de...”, clique no botão “Selecionar” que está à direita do campo “Certificado” da área “Preferências de criptografia”

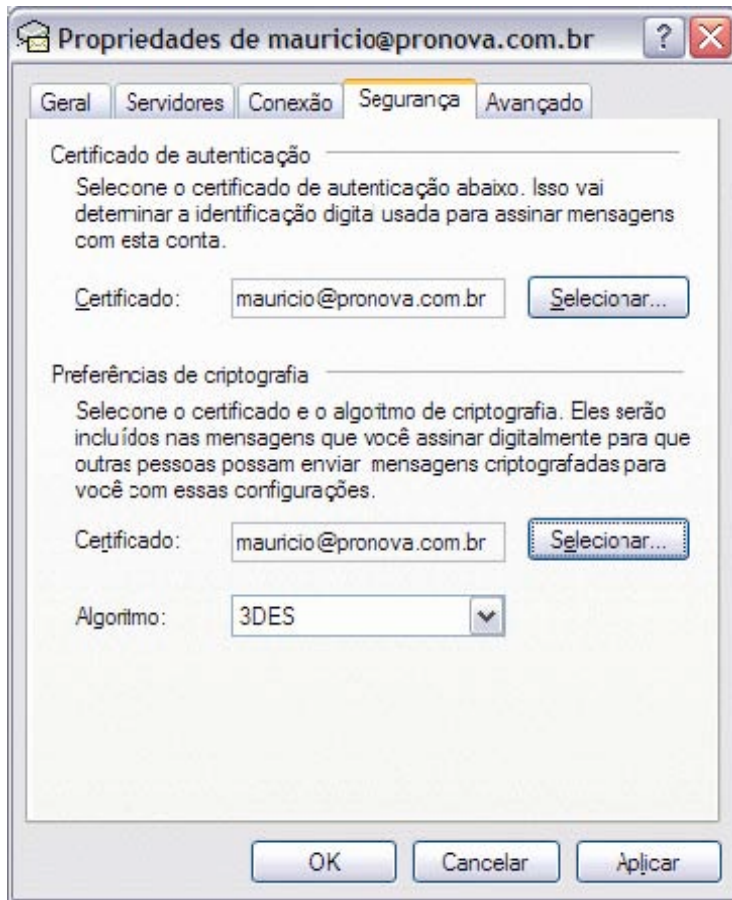


g) Na janela “Selecionar identificação digital padrão da conta”, selecione o certificado digital referente à conta em uso, em seguida clique no botão “OK”.

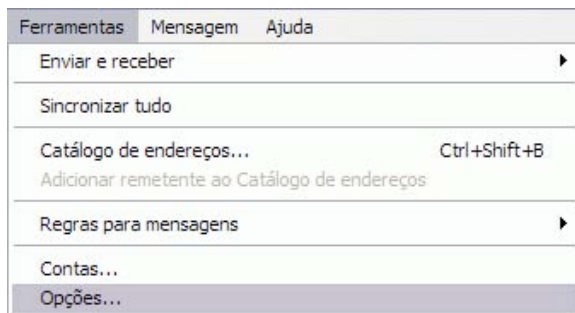


Se você deseja visualizar as informações sobre o certificado digital, clique no botão “Exibir Certificado”

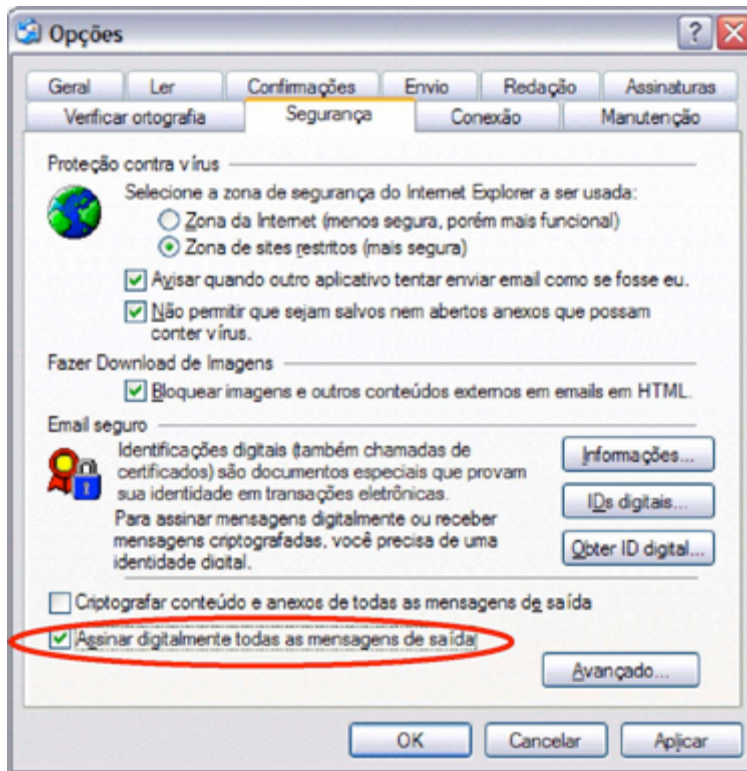
h) Agora que você informou o Outlook Express os certificados que serão utilizados para assinar e codificar (criptografar) e-mails, basta clicar no botão “OK”



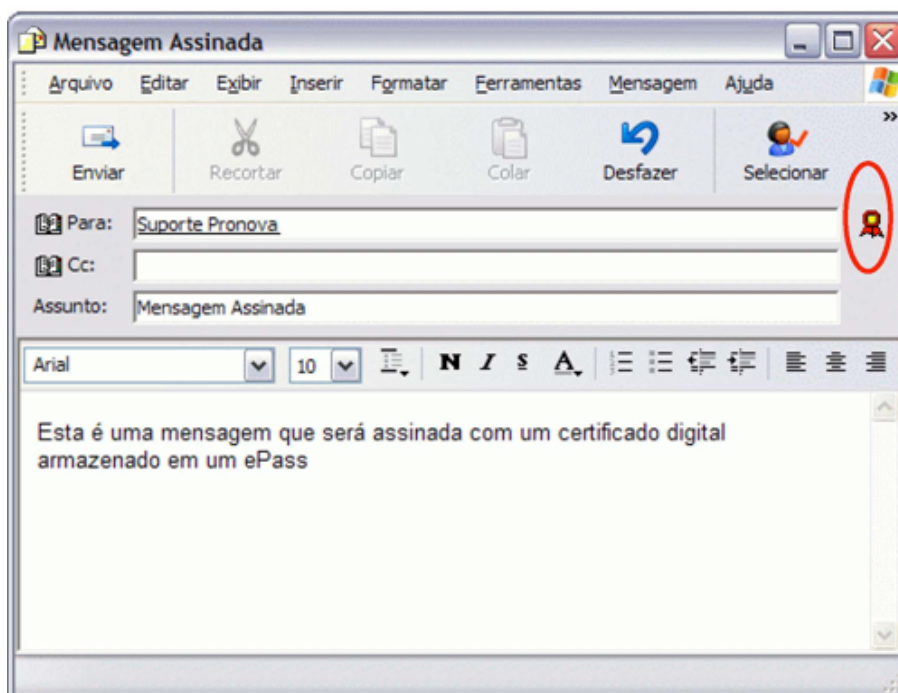
i) Clique mais uma vez em “Ferramentas” da barra de menu e depois em “Opções...”



j) Na janela “Opções”, clique na guia “Segurança”. Em seguida habilite a opção “Assinar digitalmente todas as mensagens de saída” e clique no botão “OK”



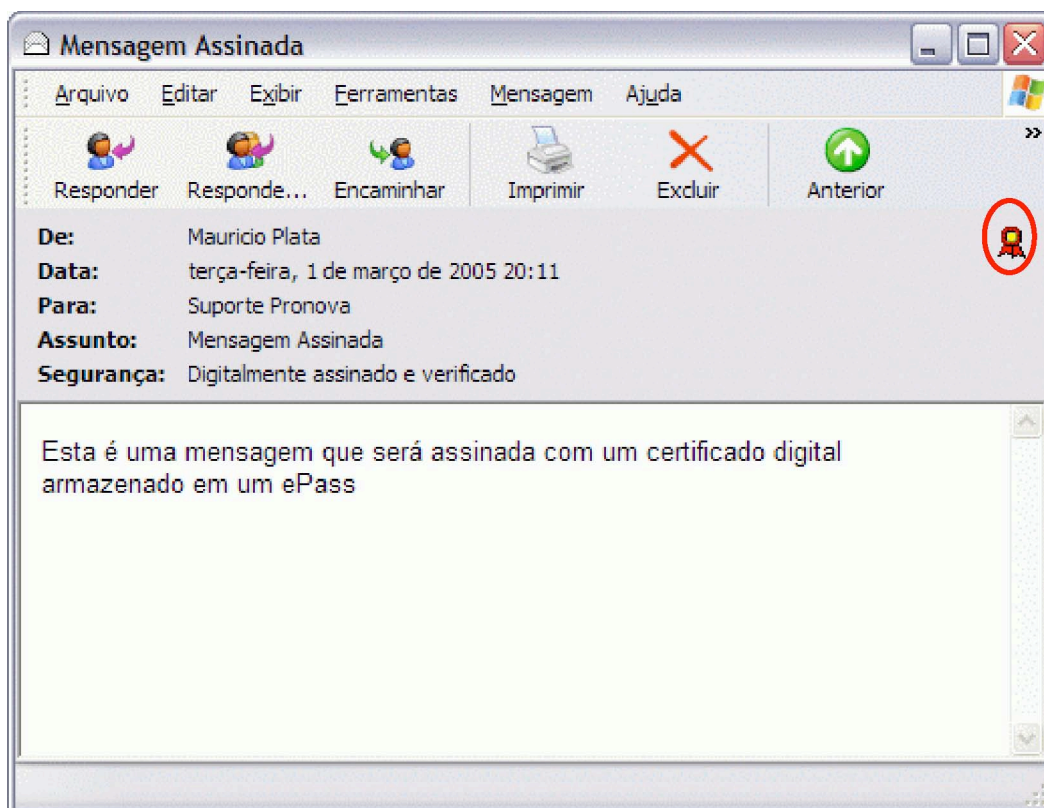
Toda vez que uma nova mensagem for criada observe que um novo ícone estará presente. Este indica que a mensagem será assinada com o certificado disponível no sistema



k) Toda vez que uma nova mensagem for criada note que um novo ícone estará presente. Este indica que a mensagem será assinada com o certificado digital da conta em uso

l) Ao clicar no botão enviar, será necessário informar o PIN do seu dispositivo. Digite-o no campo “PIN do Usuário” e depois clique no botão “Login”

m) Verifique nos itens enviados do Outlook Express se sua mensagem possui o selo indicando que a mensagem foi assinada



16. Integrando o Protoken NG com o Mozilla Thunderbird

ATENÇÃO: os procedimentos mencionados a seguir são exclusivos para este cliente de e-mail. A integração com o Microsoft Outlook e Outlook Express estão em um capítulo a parte.

Para integrar o Protoken NG com o Mozilla Thunderbird, execute os seguintes passos:

- a) Execute o Mozilla Thunderbird, clique em “Ferramentas” da barra de menu e depois em “Opções”
- b) Na janela Opções, clique em “Avançado”
- c) Em seguida, clique no sinal a esquerda de “Certificados” e depois clique no botão “Dispositivos”
- d) Uma nova janela chamada “Gerenciador de dispositivos de segurança” será exibida, clique no botão “Carregar” para continuar.
- e) Na janela “Carregar dispositivo PKCS#11”, clique no botão “Arquivo” para informar a localização do da biblioteca PKCS#11 (C:\WINDOWS\SYSTEM32\ngp11v211.dll)
- f) Ao localizar o arquivo, clique sobre o mesmo e depois no botão “Abrir”. De volta a janela “Carregar dispositivo PKCS#11, substitua “Novo módulo PKCS#11” no campo “Nome do módulo” por Protoken NG e depois clique no botão “OK”
- g) Clique no botão “OK” da janela “Confirmar”
- h) A mensagem abaixo será exibida, clique no botão “OK” para continuar.
- i) Um novo módulo Protoken NG será apresentado
- j) Clique no botão “OK” da janela “Gerenciador de dispositivos de segurança”
- k) Clique no botão “OK” da janela “Opções”

17. Configurando sua conta de e-mail no Mozilla Thunderbird para fazer uso do certificado digital armazenado no Protoken NG

- a) Execute o Mozilla Thunderbird, clique em “Ferramentas” da barra de menu e depois em “Configurar contas...”
- b) Na janela “Configurar contas”, clique na opção “Segurança” e em seguida no botão “Selecionar” da área Assinatura digital
- c) Ao clicar no botão “Selecionar” será necessário informar o PIN do seu dispositivo e depois clique no botão “OK” para continuar
- d) Na janela “Selecionar certificado” serão apresentados os detalhes do certificado armazenado no seu dispositivo. Para continuar, clique no botão “OK”
- e) O Mozilla Thunderbird irá perguntar se você deseja usar o mesmo certificado para criptografar mensagens. Se você desejar usar o mesmo certificado, clique no botão “OK”, caso contrário clique no botão “Cancelar”. No nosso guia, faremos uso do mesmo certificado, por esta razão orientamos clicar no botão “OK”
- g) Antes de concluir, recomendamos que você habilite a opção “Assinar mensagens digitalmente (por padrão)”
- h) Ainda na janela “Configurar contas”, clique no botão “Certificados” da área “Gerenciamento”
- i) Na janela “Gerenciador de certificados”, verifique se a entidade certificadora que emitiu o seu certificado digital consta da lista, caso contrário baixe o certificado da autoridade certificadora e depois clique no botão “Importar”
- j) Localize o certificado da sua Autoridade Certificadora e clique no botão “Abrir”
- k) Na janela “Efetuando o download do certificado” habilite as finalidades e clique no botão “OK”
- l) De volta a janela “Gerenciador de certificados”, clique no botão “OK” para continuar
- m) Para concluir clique no botão “OK” da janela “Configurar contas”

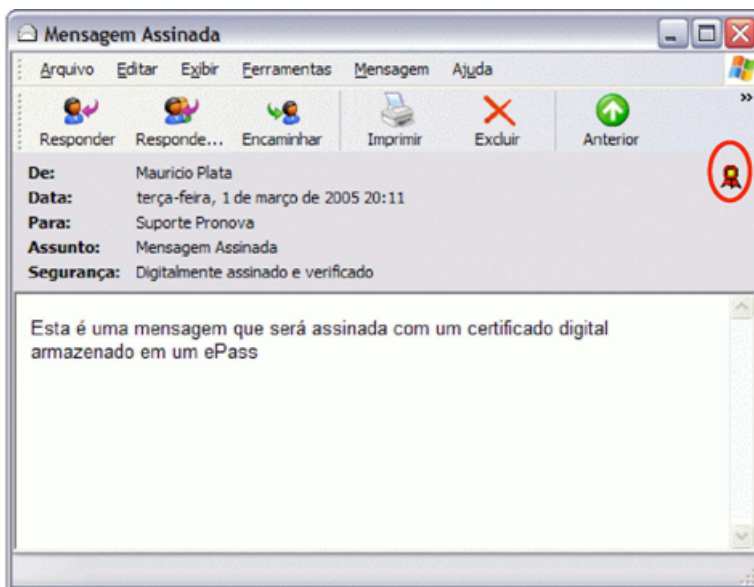
Pronto, agora o seu Mozilla Thunderbird fará uso do certificado digital armazenado no seu Protoken NG.

18. Adicionando a identidade digital do remetente ao catálogo de endereços do Windows

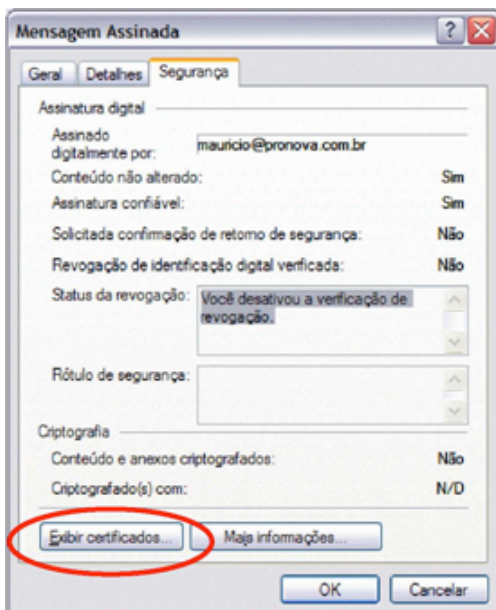
Para que seja possível a troca de e-mails criptografados, é necessário que a identidade digital da pessoa com quem você deseja trocar e-mails criptografados seja adicionada ao seu catálogo de endereços. Lembramos que não é possível trocar e-mails criptografados se uma das partes não possuir um certificado digital.

Para adicionar a identidade digital siga as seguintes instruções:

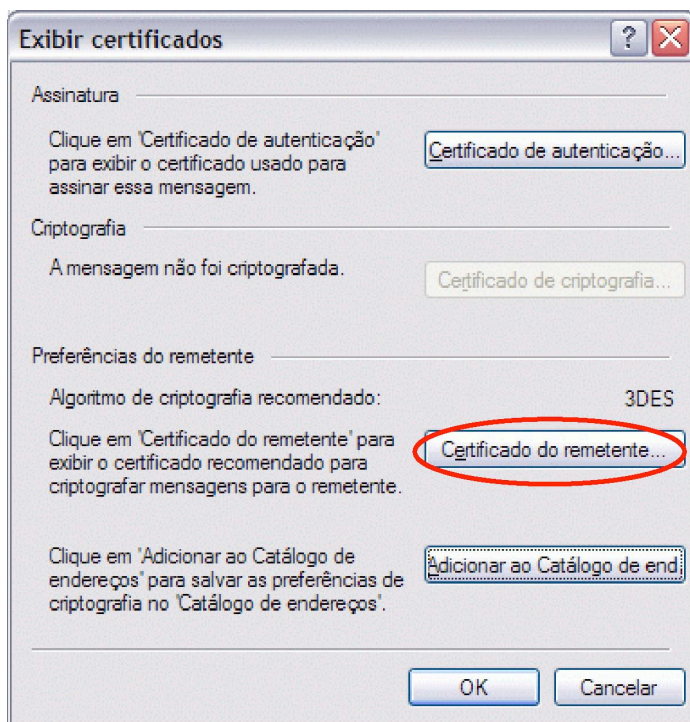
- a) Abra a mensagem assinada com um certificado digital que foi enviada pela pessoa com quem você deseja trocar mensagens criptografadas. Na janela da mensagem assinada, clique no selo.



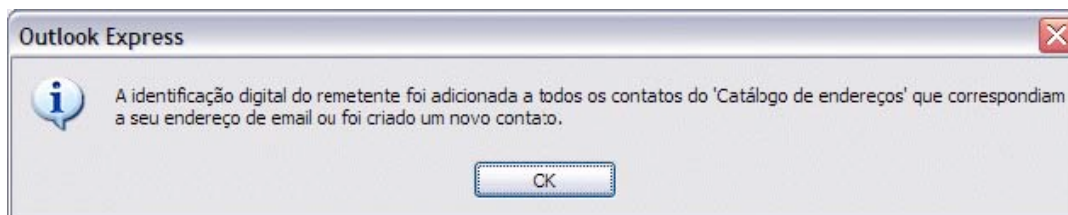
- b) A janela “Mensagem assinada” será exibida. Nesta janela, clique no botão “Exibir certificados...”



- c) Na janela “Exibir Certificados”, clique no botão “Adicionar ao Catálogo de endereços”



d) Uma janela de confirmação do Outlook Express será exibida, clique no botão “OK” para continuar

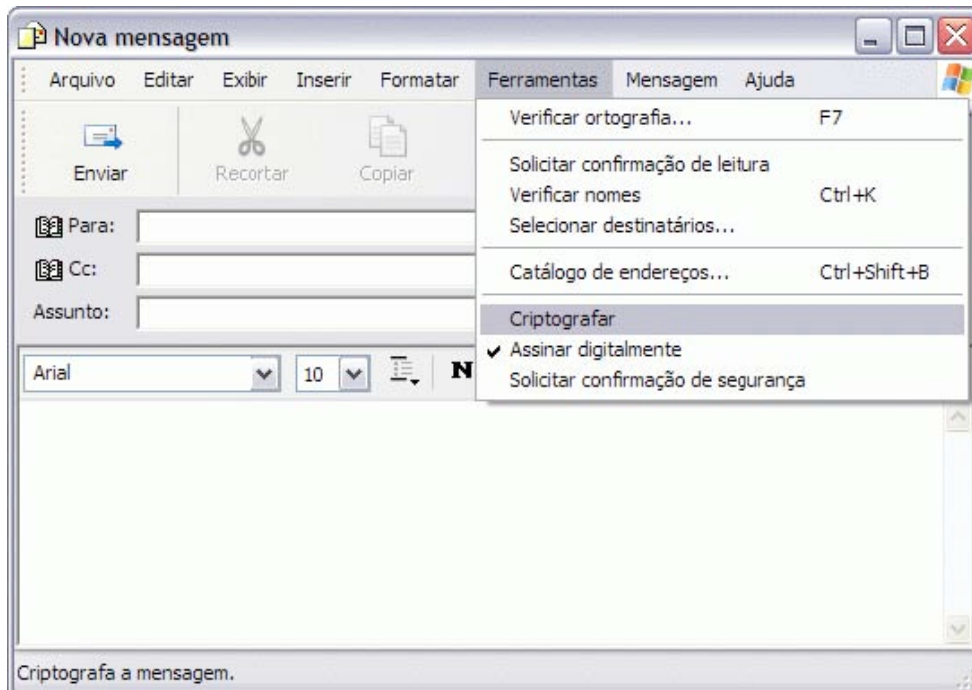


19. Enviando uma mensagem criptografada usando o Outlook Express

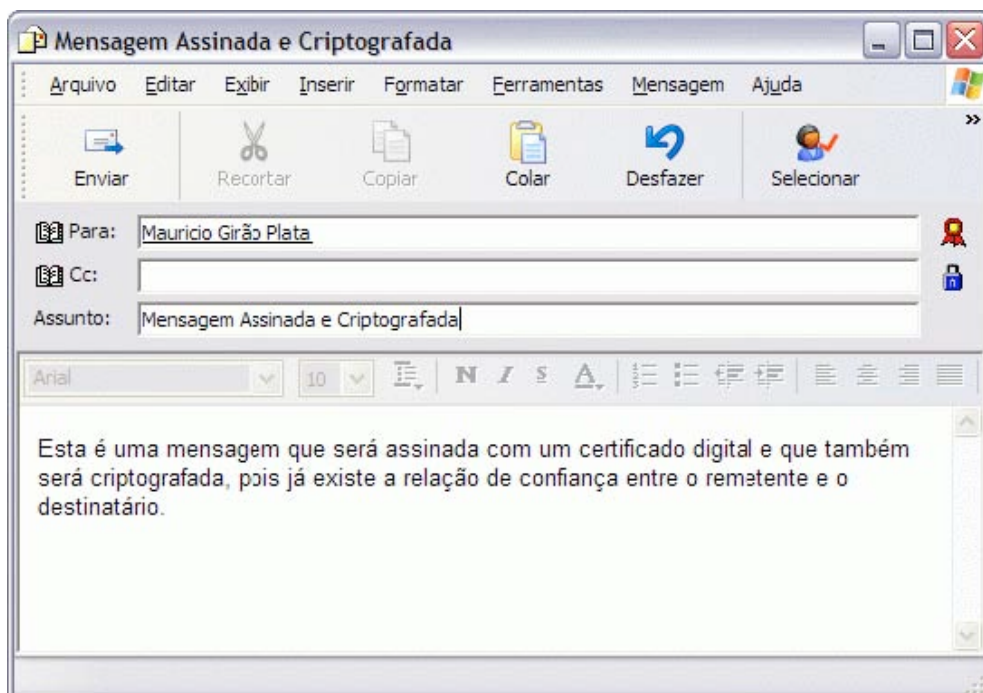
Uma vez que você adicionou a identificação digital ao catálogo de endereços, agora é possível enviar uma mensagem criptografada, como demonstraremos a seguir:

a) Crie uma nova mensagem

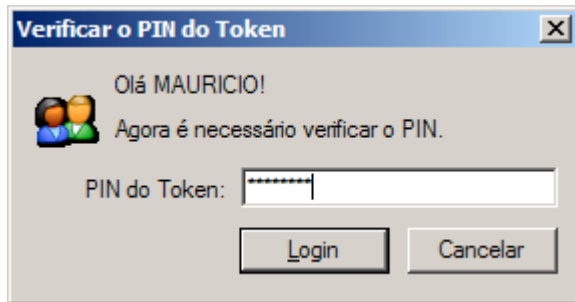
b) Clique em “Ferramentas” da barra de menu e depois selecione a opção “Criptografar”



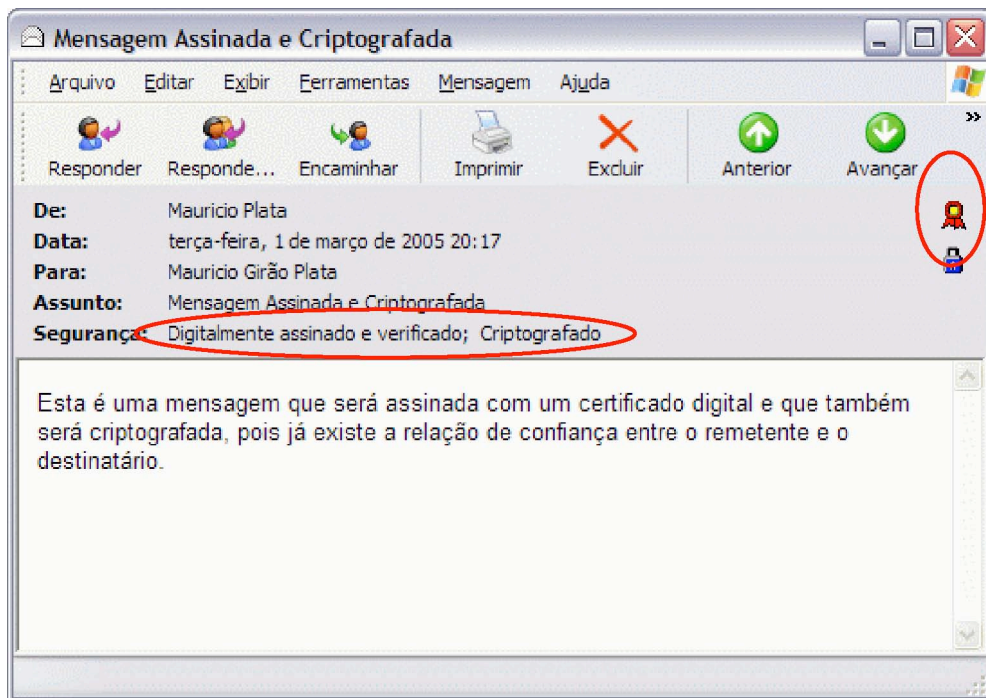
c) Note que um novo ícone será adicionado à janela. Para continuar, digite o conteúdo da mensagem, o assunto e o e-mail da pessoa que já consta no seu catálogo de endereços, a qual teve a identidade digital adicionada ao mesmo. Ao final clique no botão “Enviar”



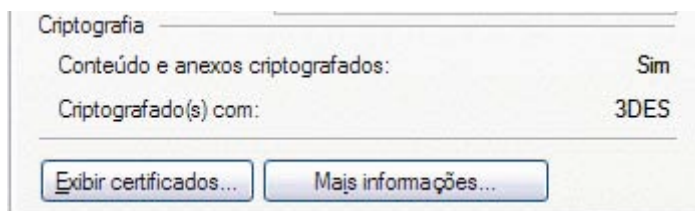
- d) Se você fechou e abriu o Outlook Express ou desconectou e conectou o seu dispositivo, será necessário informar mais uma vez o PIN do Usuário. Digite-o no campo “PIN do Usuário” e depois clique no botão “Login”



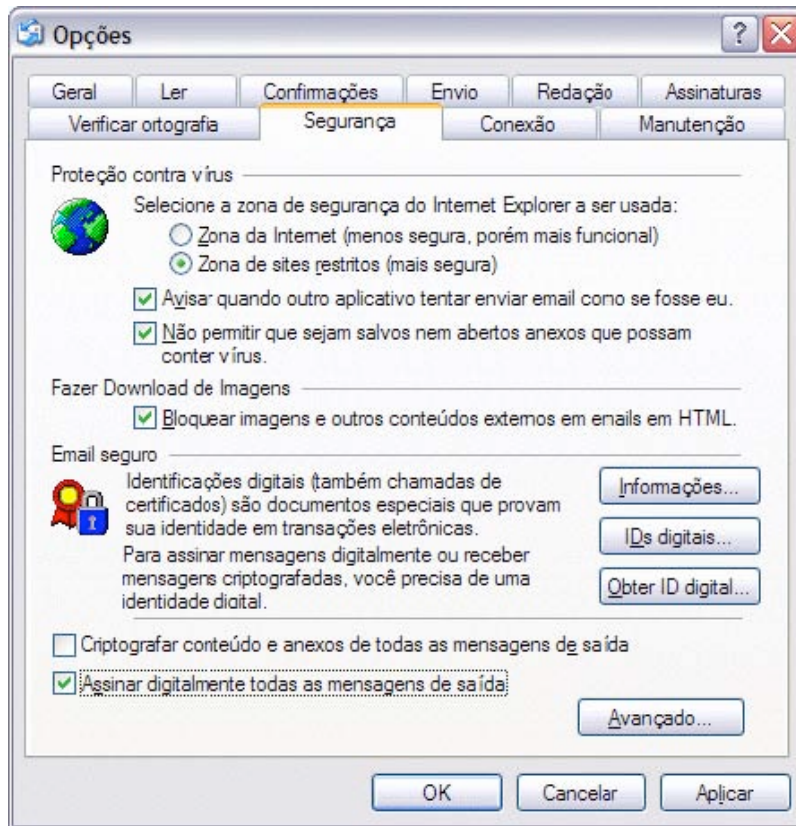
- e) A tela abaixo apresenta a mensagem enviada com os selos de assinatura e criptografia, além de uma nota informando que a mensagem está assinada digitalmente, verificada e criptografada.



- f) Ao clicar no ícone do cadeado azul uma janela com informações sobre a mensagem será exibida. Observe que a área “Criptografia” informa que o conteúdo e anexos estão criptografados e que o algoritmo utilizado foi o 3DES



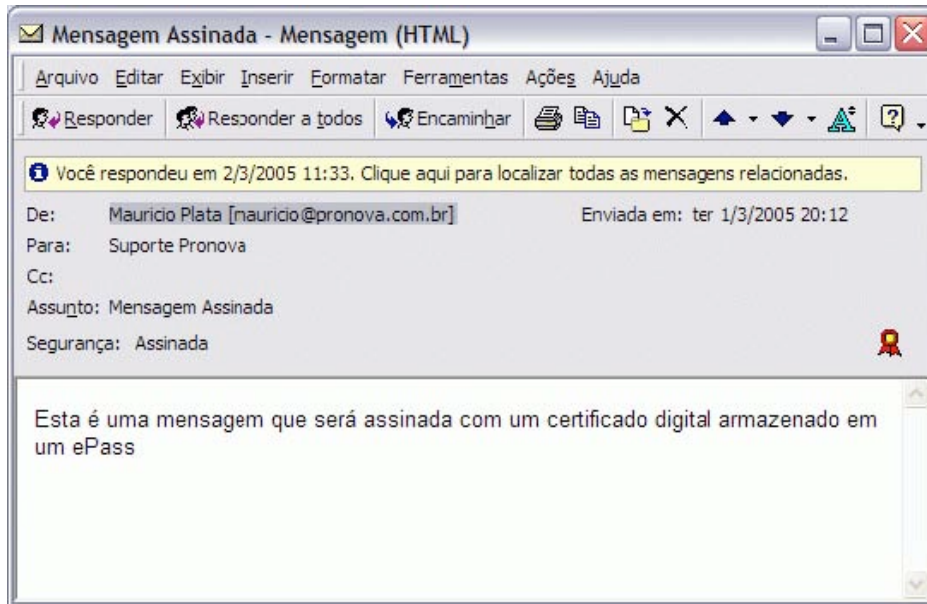
- g) Se você desejar que todas as mensagens enviadas sejam criptografadas, vá até “Ferramentas” da barra de menu depois selecione “Opções” e na janela “Opções”, habilite o item “Criptografar conteúdo e anexos de todas as mensagens de saída”



Nota: não se esqueça que para trocar mensagens criptografadas é necessário adicionar a identidade digital do destinatário ao seu catálogo de endereços.

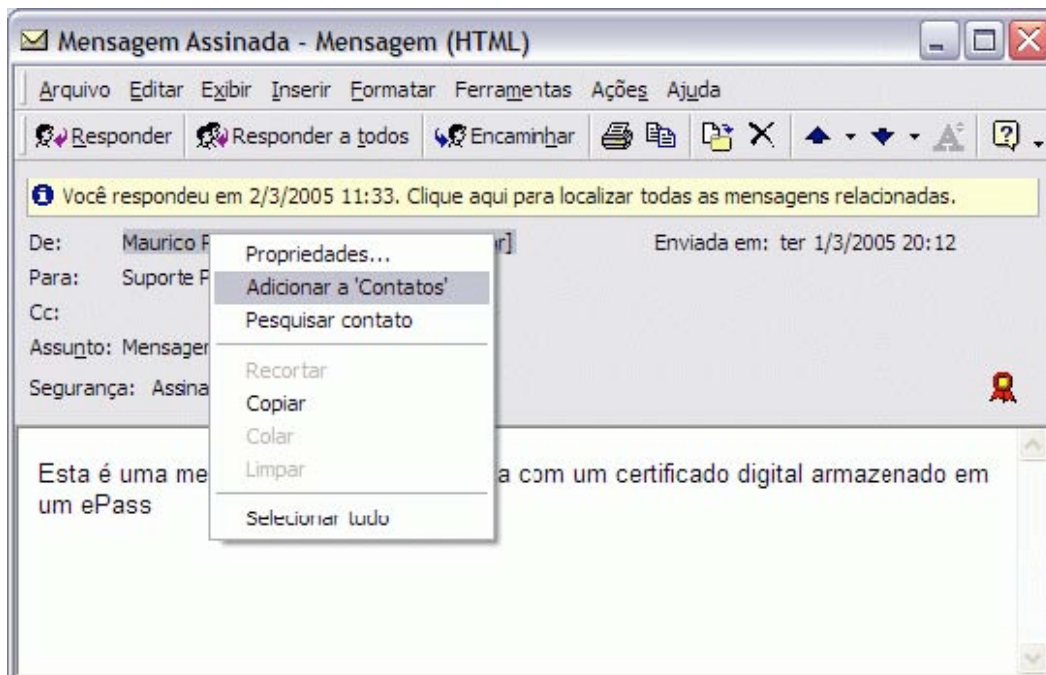
20. Adicionando uma identificação digital à sua lista de contatos do Microsoft Outlook

- a) Abra uma mensagem que tenha uma identificação digital anexada

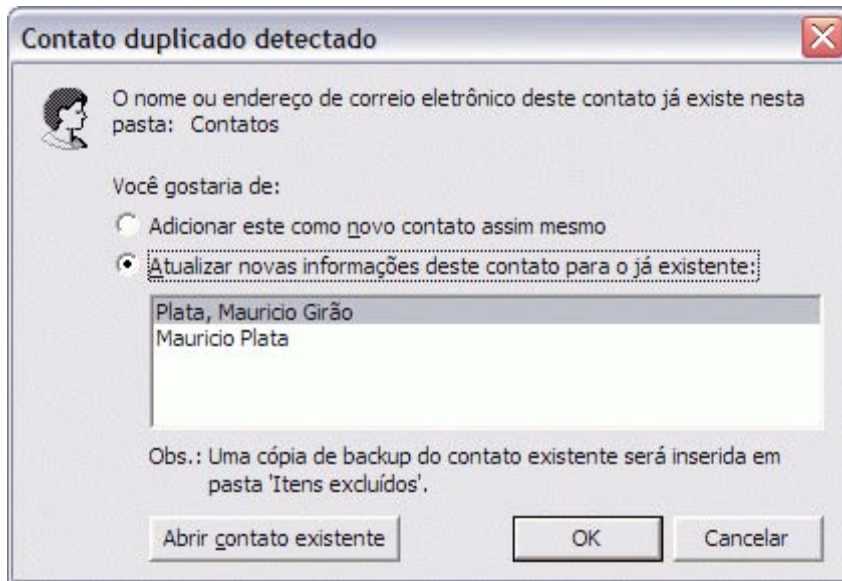


Nota: para que o remetente anexe uma identificação digital a uma mensagem, solicite que ele lhe envie uma mensagem de correio eletrônico assinada digitalmente.

- b) Clique com o botão direito do mouse no campo “De” e, em seguida, clique em “Adicionar a Contatos” no menu de atalho

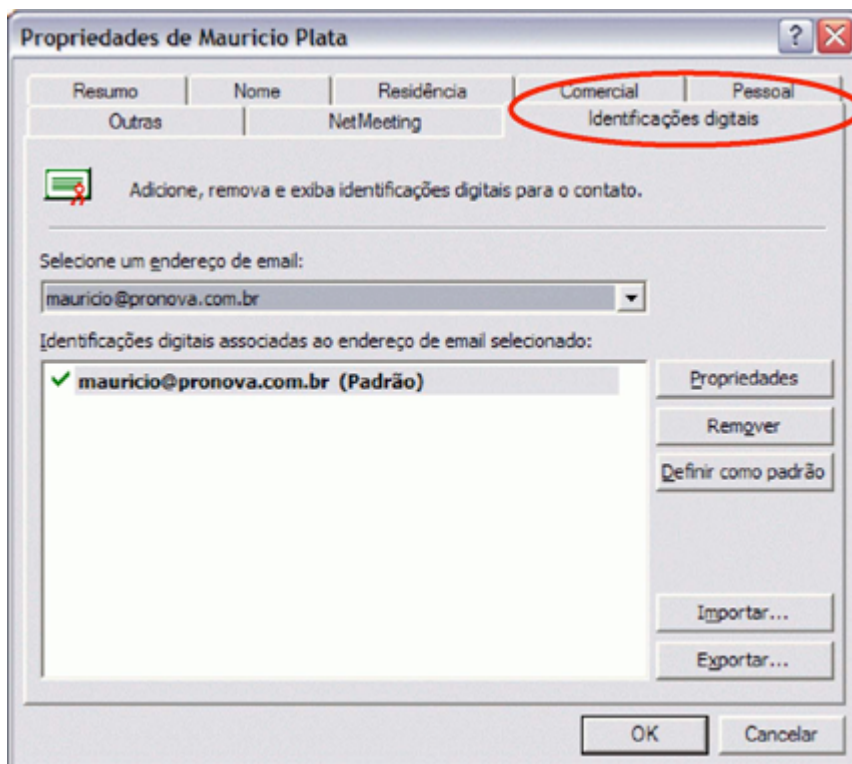


c) Se já houver uma entrada para essa pessoa na sua lista de contatos, selecione a opção “Atualizar novas informações deste contato para o já existente” e depois clique no botão “OK”



Com este procedimento a identificação digital estará agora armazenada com a sua entrada de contato para esse destinatário. Você poderá, então, enviar mensagens de correio eletrônico criptografadas para essa pessoa.

Para exibir os certificados de um contato, clique duas vezes no nome da pessoa e, em seguida, clique na guia “Identificações Pessoais”



21. Enviar uma mensagem com uma assinatura digital para um destinatário da Internet usando o Microsoft Outlook

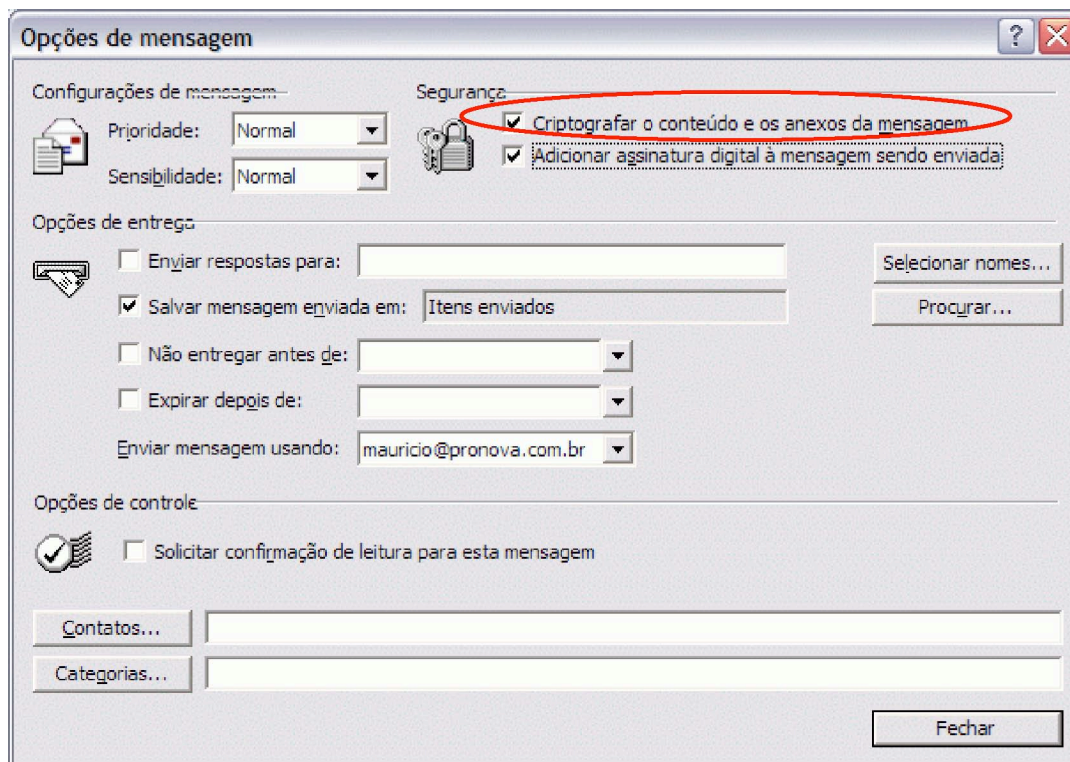
- Redija uma mensagem.
- Na mensagem, clique em “Opções”
- Marque a caixa de seleção “Adicionar assinatura digital à mensagem sendo enviada”
- Para modificar as opções de segurança para essa mensagem, clique no menu “Arquivo”, clique em “Propriedades” e, em seguida, clique na guia “Segurança”
- Habilite a opção “Adicionar assinatura digital à mensagem” e clique no botão “OK”
- De volta a mensagem, clique em “Enviar”.

Observação:

- Para adicionar uma assinatura digital a todas as mensagens que você envia, clique no menu “Ferramentas” na janela principal do Outlook, clique em “Opções” e, em seguida, na guia “Segurança”. Marque a caixa de seleção “Adicionar assinatura digital a mensagens sendo enviadas”.

22. Enviar uma mensagem criptografada para um destinatário da Internet usando o Microsoft Outlook

- Redija uma mensagem.
- Na mensagem, clique em “Opções”. Marque a caixa de seleção “Criptografar o conteúdo e os anexos da mensagem”



- Clique em “Enviar”.

Observações:

- Para criptografar todas as mensagens enviadas, no menu “Ferramentas”, clique em “Opções” e, em seguida, clique na guia “Segurança”. Marque a caixa de seleção “Criptografar conteúdo e anexos de mensagens sendo enviadas”.
- Para modificar as configurações de segurança de uma mensagem específica, clique no menu “Arquivo” na janela de mensagens e, em seguida, clique em “Propriedades”.

23. Removendo o software do Protoken NG

Para remover o software do Protoken NG, vá até o Pannel de Controle “Adicionar ou Remover Programas”, localize a opção “Protoken NG (Somente remover)” e clique no botão “Alterar / Remover” e siga as instruções do assistente.

24. Perguntas e Respostas Comuns

- a) Ao tentar formatar o meu dispositivo recebo a mensagem “Desculpe, mas o PUK informado está incorreto” O que pode estar errado?

R: Esta mensagem é exibida, pois PUK informado não é o correto. Para formatar o Protoken NG, é necessário informar o atual PUK no campo “Digite o ATUAL PUK do Token” da janela “Formatar o Token (Inicializar Setor PKI)”. Tenha cuidado para não informar cinco vezes o valor errado do PUK, pois se você fizer isso, o seu Protoken NG será bloqueado. Para desbloqueá-lo será necessário reformatá-lo, perdendo-se assim todas as informações que estão armazenadas nele.

Nota: se você não possui o PUK do seu dispositivo, entre em contato com o Administrador de Sistemas da sua empresa. Lembramos que existe um número pré-determinado de tentativas de acerto do PUK. Se estas forem excedidas o seu dispositivo será bloqueado e todo o conteúdo do dispositivo ficará indisponível.

- b) O botão “OK” da janela ‘Formatar Token’ não está disponível para uso. O que pode estar errado?

R: Verifique os valores digitados nos campos “Digite um NOVO PIN” e “Confirme o NOVO PIN”, certamente eles não possuem o mesmo valor ou tamanho.

- c) Tenho um certificado digital ICP-Brasil no meu dispositivo, mas não consigo fazer uso em aplicações no Internet Explorer. O que pode estar errado?

R: Certamente o seu navegador não possui a cadeia de certificados da ICP-Brasil e da Autoridade Certificadora que emitiu o seu certificado digital. Para resolver este problema, é necessário proceder a instalação da cadeia de certificados, consulte a equipe de suporte da sua Autoridade Certificadora para conhecer os procedimentos de instalação da cadeia de certificados. Se você não tem acesso a Internet, use o diretório ICP-Brasil do CD-ROM de instalação do seu Protoken NG. Nele colocamos os arquivos de cadeia de certificado da grande maioria de ACs credenciadas à ICP-Brasil

- d) Ao conectar o meu Protoken NG na porta USB, a luz dele fica piscando ele não é reconhecido. O que pode estar errado?

R: Certamente o software do Protoken NG não está instalado, execute o arquivo runtime.exe que está na raiz do CD-ROM e siga as instruções do instalador. Maiores detalhes poderão ser encontrados no Tópico 4 “Instalando o software do Protoken NG”.

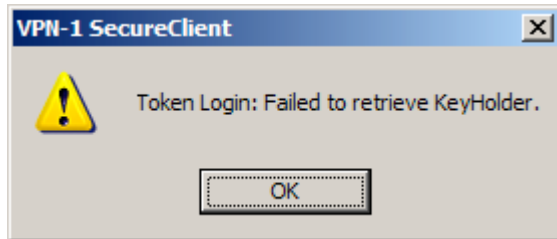
Se o problema persistir, verifique se a controladora USB do seu micro está habilitada na BIOS da sua placa-mãe.

- e) Ao conectar o meu Protoken NG na porta USB, a luz dele não liga ele não é reconhecido. O que

pode estar errado?

R: Certamente a porta USB do seu computador não está instalada fisicamente. Consulte um técnico para fazer a verificação desta porta USB ou tente conectar o seu Protoken NG em um outro computador. Se o problema persistir entre em contato com a Pronova.

- f) O Cliente VPN-1 SecuRemote da Check Point não consegue localizar o meu certificado que está armazenado no Protoken NG. Se eu insisto, o cliente SecuRemote consegue identificar, mas ao selecionar o certificado ele exibe a mensagem “Token Login: Failed to retrieve KeyHolder”. O que pode estar errado?



R: Este é um problema clássico de ausência do caminho (path) da autoridade certificadora que emitiu o seu certificado. Sem esta informação, certamente o seu certificado é tratado pelo sistema operacional como um certificado inválido. Para resolver este problema, basta instalar o certificado raiz da autoridade certificadora no repositório do Windows ou importar para o Protoken NG o certificado raiz da AC que emitiu o seu certificado digital.

- g) Travei o PUK do meu Protoken NG, perdi o meu dispositivo?

R: Não, você não perdeu o seu dispositivo. Todavia, para reativar o acesso ao seu Protoken NG, será necessário reinicializar o seu equipamento para as condições originais de fábrica. Em outras palavras, ao usar a ferramenta ePassNG_Init.exe que está no diretório “ePassNG_Init”, todas as informações que estiverem armazenadas no seu ePass200 serão apagadas. Maiores instruções sobre a utilização desta ferramenta poderão ser encontradas no documento ePassNG_Init.pdf que está no mesmo diretório desta ferramenta.

- h) Posso instalar mais de um certificado no meu Protoken NG?

R: Sim, você poderá instalar mais de um certificado no seu Protoken NG, mas tenha em mente que existe uma limitação que é a quantidade de memória do seu dispositivo (32K). Normalmente conseguimos colocar até 05 (cinco) ou 06 (seis) certificados. Observe ainda que você se você usar seu certificado para codificar mensagens e/ou documentos talvez você terá que guardar este seu certificado por um tempo após a expiração deste, para que seja possível a decodificação destes dados.

Tendo em vista que a chave privada gerada no Protoken NG não pode ser exportada, recomendamos que não sejam armazenados no mesmo Protoken NG, certificados que não tenham relação entre si. Por exemplo, um certificado e-CNPJ de uma empresa X mais um certificado e-CNPJ de uma empresa Y. Imagine que a empresa X deseja ter com ela o seu certificado. Como a chave privada é parte integrante do certificado e-CNPJ, para resolver este impasse será necessário revogar o certificado da empresa X. A seguir fazer uma nova aquisição de um e-CNPJ para a empresa X em outro Protoken NG.

- i) O Protoken NG pode ser utilizado em outros sistemas operacionais?

R: Sim, o Protoken NG poderá ser utilizado nos sistemas operacionais Linux ou Mac. O software necessário para instalar o Protoken NG nestes sistemas operacionais poderá ser encontrado nos diretórios Linux e Mac do CD-ROM de instalação do Protoken NG.

25. Suporte Técnico

Se as informações contidas neste guia rápido não foram suficientes, não se preocupe, entre em contato conosco sempre que precisar. Nosso e-mail para suporte é suporte@pronova.com.br, o telefone para contato é (21) 2491-3688 e o nosso chat está em www.pronova.com.br.

26. Contatos

Pronova Soluções Inteligentes (Distribuidor Autorizado)

Endereço	Av. das Américas 500, bloco 4 (entrada A), Sala 302. Barra da Tijuca. Rio de Janeiro – RJ. CEP 22.640-100. Brasil.
Telefones	+55-21-24913688
Fax	+55-21-24913688 (ramal 103)
E-mail	suporte@pronova.com.br ou sac@pronova.com.br
Sites	www.pronova.com.br ou www.lojapronova.com.br

Feitian Technologies Inc., Ltd. (Fabricante)

Endereço	3Fl., No.5 Building, Jimen Hotel, Xueyuan Road, Haidian District, Beijing, 100088, República Popular da China
Telefones	+86-10-62360800 e +86-10-62360900
Fax	+86-10-82070027
Site	www.FTsafe.com